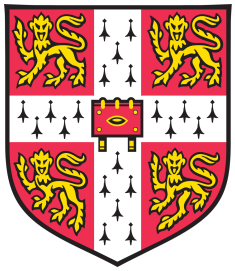
Computing the Cassels-Tate Pairing

Monique van Beek



University of Cambridge
Department of Pure Mathematics and Mathematical Statistics
Lucy Cavendish College

August 2015

This dissertation is submitted for
the degree of Doctor of Philosophy

Abstract

For an elliptic curve E admitting a p-isogeny $\phi : E \to \hat{E}$ we calculate the Cassels-Tate pairing on $S^{(\hat{\phi})}(\hat{E}/K) \times S^{(\hat{\phi})}(\hat{E}/K)$ using a pushout form. We calculate examples in the $p = 3$ case of type μ_3-nonsplit, $\mathbb{Z}/3\mathbb{Z}$-nonsplit and generic 3-isogeny. In the $p = 5$ case, we calculate examples on curves with a rational 5-torsion point. We use this pairing to search for high-rank curves in families of elliptic curves having torsion group isomorphic to either $\mathbb{Z}/9\mathbb{Z}$ or $\mathbb{Z}/12\mathbb{Z}$, and discover two new curves of rank 4 in the former case. We also show how to use the pushout form method to calculate the pairing on $S^{(p)}(E/K) \times S^{(\phi)}(E/K)$.

In the course of our calculations, many norm equations needed to be solved. We give a new algorithm for solving norm equations in cubic extensions. This algorithm is shown always to terminate when the base field is $\mathbb{Q}$.

Declaration

This dissertation is the result of my own work and includes nothing which is the outcome of work done in collaboration except as declared in the Preface and specified in the text.
It is not substantially the same as any that I have submitted, or is being concurrently submitted for a degree or diploma or other qualification at the University of Cambridge or any other University or similar institution except as declared in the Preface and specified in the text. I further state that no substantial part of my dissertation has already been submitted, or is being concurrently submitted for any such degree, diploma or other qualification at the University of Cambridge or any other University of similar institution except as specified in the text

Monique van Beek
October 26, 2015

Acknowledgements

My deepest gratitude to my supervisor, Tom Fisher, for his ever patient guidance. I also thank my office mate Anton Isopoussu for many interesting mathematical conversations, and my parents for their continuing support and encouragement, both financial and otherwise. I acknowledge the financial support of Lucy Cavendish College and the Department of Pure Mathematics and Mathematical Statistics.

Contents

Chapter 1

Introduction

Let E be an elliptic curve over some number field K. By the Mordell-Weil theorem, the rational points $E(K)$ form a finitely generated abelian group. The number of points needed to generate the nontorsion part of $E(K)$ is called the rank. Determining the rank of $E(K)$ is a nontrivial problem, and there is no known algorithm that will compute $E(K)$ in all cases. In this thesis, we are mainly concerned with determining upper bounds on the ranks of various elliptic curves over $\mathbb{Q}$.

Because working with $E(K)$ directly is problematic, we also consider the Tate-Shafarevich group $Ш(E/K)$, introduced by Lang, Tate and Shafarevich in [LT58, Sha59]. This is a group associated to E consisting of the set of torsors of E which have points everywhere locally. It is known that $Ш(E/K)$ is torsion, and it is conjectured that it is a finite group. Cassels showed that if it is finite, then its order is a square [Cas62]. This is not the case in general. In [PS98], Poonen and Stoll show that in the case of A an abelian variety, $Ш(A/K)$ is not always a square, even when A is the Jacobian of a curve over a number field. In the proof of the Mordell-Weil theorem, the rank is bounded by considering $E(K)/nE(K)$ for any $n \geq 2$. The upper bound found in this way can be improved whenever we find that $Ш(E/K)$ contains nontrivial n-torsion.

We will thus want to calculate the Selmer group $S^{(n)}(E/K)$, which consists of all n-coverings of E that have points everywhere locally. It is part of the following short exact sequence.

$$0 \longrightarrow E(K)/nE(K) \longrightarrow S^{(n)}(E/K) \longrightarrow Ш(E/K)[n] \longrightarrow 0$$

For certain E, it is possible to calculate $S^{(n)}(E/K)$ indirectly by considering some isogeny $\phi : E \to \hat{E}$ of degree n and using the Selmer groups associated to it. Calculations to compute these various Selmer groups are known as descent calculations.

In our case, we will be considering the n-isogeny

$$\phi : E \longrightarrow \hat{E}$$

with dual $\hat{\phi} : \hat{E} \to E$ such that $\phi \circ \hat{\phi} = [n]$, the multiplication-by-$n$ map. The Selmer group $S^{(\phi)}(E/K)$ consists of all ϕ-coverings of $\hat{E}$ that have points everywhere locally and is part of the following short exact sequence

$$0 \longrightarrow \hat{E}(K)/\phi E(K) \longrightarrow S^{(\phi)}(E/K) \longrightarrow Ш(E/K)[\phi] \longrightarrow 0.$$

We will follow Cassels [Cas62] and define a pairing

$$< , >: Ш(E/K) \times Ш(E/K) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

with the property that $y \in Ш(E/K)$ is in the image of $\hat{\phi} : Ш(\hat{E}/K) \to Ш(E/K)$ if and only if y pairs trivially with every element in the kernel of $\phi : Ш(E/K) \to Ш(\hat{E}/K)$. This pairing is called the Cassels-Tate pairing. It lifts naturally to a pairing on Selmer groups, which is what we will be computing in this thesis. This allows us to turn a ϕ-descent calculation into a full n-descent, thus potentially improving the upper bound on the rank.

Many others have worked on computing the Cassels-Tate pairing, and we name some results here. The first was Cassels [Cas59, Cas62]. He not only defined the pairing but computed it in a numerical example. He showed that the curve given by

$$C : x^3 + y^3 + 5610z^3 = 0$$

contained no rational points other than $(1,-1,0)$ by considering a 3-isogeny $\phi : C \to \hat{C}$ and computing the pairing on $S^{(\phi)}(C/\mathbb{Q})$. Cassels used the pairing in [Cas98] to turn a 2-descent into a 4-descent. Donnelly has implemented the Cassels-Tate pairing between 2-coverings fully in MAGMA [Don]. For $p = 3$ or 5, the pairing on the p-Selmer group of an elliptic curve $E/\mathbb{Q}$ with $E[p] \cong \mu_p \times \mathbb{Z}/p\mathbb{Z}$ was calculated in [Fis03]. In [Cas64], Cassels uses the Cassels-Tate pairing to show that for some elliptic curves $E/\mathbb{Q}$ the 3-part of $Ш(E/\mathbb{Q})$ can be arbitrarily large. Bölling in [Böl75] and McGuinness in [McG82] used the pairing on $Ш(E/\mathbb{Q})[2]$ to demonstrate that there are elliptic curves E defined over $\mathbb{Q}$ such that the 2-rank of $Ш(E/\mathbb{Q})[2]$ is arbitrarily large.

Chapter 2 contains all the background information pertaining to descent calculations we will need. This chapter also contains formulae for bounding the rank. We pay most attention to the case of descent by 3-isogeny, as this will be the main focus of this thesis.

Chapter 3 defines the Cassels-Tate pairing, giving two definitions, both of which define the same pairing. The most important definition is the pushout function definition, for this is the definition we have used to write a program to compute the pairing in a variety of cases when E admits certain kinds of 3-isogeny. Section 3.5 gives equations for the pushout form that is used. Unfortunately, many of the forms had very large coefficients, therefore we omit them from most of the examples in this thesis. Instead, we provide the necessary parameters to plug into these formulae.

During the course of our calculations, we came across many norm equations of the form $N_{L/K}(\xi) = b$, where L is a cubic extension of some number field. K. For most of the interesting examples we wanted to calculate, the MAGMA function `NormEquation` was insufficient for our purposes. Chapter 4 therefore contains an algorithm inspired by [Cre99]. When $K = \mathbb{Q}$, we have an algorithm that we have proved always terminates. For extensions of large discriminant, the gains made by this algorithm are considerable, often giving an answer when `NormEquation` failed to terminate at all. The algorithm involves an iterative procedure whereby we associate a binary cubic form to the norm equation. This form is then reduced according to some definition of what a 'reduced' cubic looks like, and the result is used to set up a new norm equation to solve, this time over a smaller field extension. We have also implemented the algorithm for K a small imaginary quadratic extension of $\mathbb{Q}$. We cannot prove that it works in all cases, but we have used it successfully nonetheless in examples.

In Chapter 5, we demonstrate two of the methods that were defined in Chapter 3 to compute the Cassels-Tate pairing. The difference between them depends mostly on whether one wants to find local points on the elliptic curve E itself or on the coverings of E. We choose to continue with one of these methods in Chapter 6, in which we apply our methods to three families of elliptic curves. Section 6.1 demonstrates that at present there is no known example of an elliptic curve with torsion group $\mathbb{Z}/3\mathbb{Z}$ and rank greater than 13. The goal in Sections 6.2 and 6.3 is to find new high rank curves in two families. We were partly successful in this, as we found many new curves with torsion group $\mathbb{Z}/9\mathbb{Z}$ and rank 3, and a few curves

with rank 4, which is the highest rank in this family so far.

In Chapter 7, we explore further methods for refining the upper bound on the rank. This is done by calculating the Cassels-Tate pairing on the Selmer groups $S^{(\phi)}(E/\mathbb{Q}) \times S^{(3)}(E/\mathbb{Q})$ in order to turn the 3-descent into a 3ϕ-descent. This method is then applied to one of the candidates for high rank curves we found in Chapter 6.

Chapter 8 shows how our calculations can be generalised to $p = 5$, in the case that we have an elliptic curve with a rational torsion point of order 5. Although we can do some examples, the greatest bottleneck in our computations is in solving norm equations, and unfortunately we were not able to generalise the work done in Chapter 4.

1.1 Selmer's Famous Example

As a motivating example, we consider three methods to see that Selmer's famous example

$$F(x_1,x_2,x_3) = 3x_1^3 + 4x_2^3 + 5x_3^3 = 0 \tag{1.1}$$

violates the Hasse principle. First we show this by a direct calculation, as done by Selmer in [Sel51]. Next we consider a 2-descent, and finally we use the material to be covered in this thesis.

Selmer's Method

We show that (1.1) has points everywhere locally but no global solution, as done by Selmer in [Sel51]. First we note that if there is a global solution, then there must be a solution with the following pairwise coprime integers.

$$\mathrm{GCD}(x_1,x_2) = \mathrm{GCD}(x_1,x_3) = \mathrm{GCD}(x_2,x_3) = 1 \tag{1.2}$$

We now need to show that there is a local solution for every prime p. For any prime p dividing one of the coefficients of F, the following table gives a point P modulo p that lifts to a local point in $\mathbb{Q}_p$.

p	$P \pmod p$
2	$(1,0,1) \pmod 2$
3	$(0,2,2) \pmod 3$
5	$(3,1,0) \pmod 5$

In all other cases, we can lift any solution of $F(x_1,x_2,x_3) \equiv 0 \pmod p$ to a solution in $\mathbb{Q}_p$. This is because at least one of the following must be nonzero modulo p.

$$\frac{\partial F}{\partial x_1} = 9x_1^2 \qquad \frac{\partial F}{\partial x_2} = 12x_2^2 \qquad \frac{\partial F}{\partial x_3} = 15x_3^2 \tag{1.3}$$

Thus we need only find a solution to $F(x_1,x_2,x_3) \equiv 0 \pmod p$ for every remaining p.

By the Hasse-Weil bound, for any curve C of genus g we have

$$\#C(\mathbb{F}_p) \geq p + 1 - 2g\sqrt{p}.$$

Thus any smooth curve of genus 1 will always contain an $\mathbb{F}_p$ point. The following is an overview of Selmer's method to arrive at this same conclusion.

If $p \equiv -1 \pmod 3$, every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cubic residue, thus a suitable solution always exists.

If $p \equiv 1 \pmod 3$, the situation is more complicated. If $p = 7$, we can Hensel lift $(1,1,0) \pmod 7$ to a solution in $\mathbb{Q}_7$. If $p > 7$ the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ fall into one of three classes: the class of cubic residues A or one of the two classes of nonresidues A' and A''. The rules of multiplication are given by the following table.

	A	A'	A''
A	A	A'	A''
A'	A'	A''	A
A''	A''	A	A'

If two of the coefficients of F fall into the same class, then we can easily find a solution. For example, if 3 and 4 are in the same class, then we find that $3^3 \cdot x_1^3 + 3^2 \cdot 4 \cdot x_2^3 \equiv 0 \pmod p$ must have a solution as we must have $3^2 \cdot 4 \in A$. Thus we need only consider the case that $3, 4$ and 5 all lie in different classes. Thus we need to show that there exist a, a', a'' in the three different classes such that

$$a + a' = a'' \pmod p. \tag{1.4}$$

To do this, we add 1 to each element of A. Denote by α, β, γ the number of elements that end up in A, A', A'' respectively. Define α', β', γ' by adding 1 to each element of A' and noting how many elements end up in A, A', A'' respectively. Define $\alpha'', \beta'', \gamma''$ similarly. Thus we find

$$\alpha' + \beta' + \gamma' = \alpha'' + \beta'' + \gamma'' = \frac{p-1}{3}, \tag{1.5}$$

the number of elements in each class. However, because $-1 \in A$, we find

$$\alpha + \beta + \gamma = \frac{p-1}{3} - 1. \tag{1.6}$$

For any element $a' \in A'$ such that $a' = 1 + a$ for some $a \in A$, we have that $-a = -a' + 1$. We know that $-a \in A$ and $-a' \in A'$, thus we have $\alpha' = \beta$. Multiplication by $(-a')^{-1}$, which lies in A'', gives us an element of A'' which is the sum of 1 with another element of A'', thus

$$\beta = \alpha' = \gamma''$$

and by a similar argument we find

$$\gamma = \beta' = \alpha''.$$

Thus from (1.5) and (1.6) we find

$$\gamma' = \beta'' = \alpha + 1 \geq 1.$$

Thus $a'' = 1 + a'$ for at least one pair a', a'', which is what we were looking for in (1.4). We have shown there exists a local solution for every p.

Now we show there is no global solution. By a simple rescaling, we see that (1.1) has a rational solution if

$$C : X^3 + 6Y^3 = 10Z^3 \tag{1.7}$$

has some nontrivial integer solution for pairwise coprime X,Y,Z. Let $K=\mathbb{Q}(\alpha)$ where $\alpha^3=6$. Then K has class number 1 and (1.7) decomposes into

$$(X+Y\alpha)(X^2-XY\alpha+Y^2\alpha^2)=(\alpha-2)^3(\alpha-1)(\alpha^2-2\alpha+1)(Z)^3.$$

Assume there is some prime ideal $\mathbf{p}$ such that $\mathbf{p}|(X+Y\alpha)$ and $\mathbf{p}|(X^2-XY\alpha+Y^2\alpha^2)$. Since $X^2-XY\alpha+Y^2\alpha=(X+Y\alpha)^2-3XY\alpha$ we also find $\mathbf{p}|(3XY\alpha)$. If $\mathbf{p}|(3)$, then because $\mathbf{p}|(Z)^3$ we must have $3|Z$ which implies $3|X$, contradicting the coprimality of X and Z. If $\mathbf{p}|Y$, then we must also have $\mathbf{p}|X$, violating the pairwise coprime property. Similarly, if $\mathbf{p}|X$, we must have either $\mathbf{p}|Y$ or $\mathbf{p}|(\alpha)$, thus we find that we must have $\mathbf{p}|(\alpha)$. It follows that we must have $\mathbf{p}=\mathbf{p}_2=(\alpha-2)$, the only prime ideal lying over 2.

We have that 5 splits into two ideals, $(5)=\mathbf{p}_5\mathbf{p}_{25}=(\alpha-1)(\alpha^2-2\alpha+1)$. Looking at (1.7) modulo 5, we see $X\equiv -Y \bmod 5$, so $\mathbf{p}_5|(X+Y\alpha)$. If also $\mathbf{p}_{25}|(X+Y\alpha)$, then $5|X$ and $5|Y$, contradicting the relative coprime condition. Thus $\mathbf{p}_{25}|(X^2-XY\alpha+Y^2\alpha^2)$. Thus far we have

$$\begin{aligned}(X+Y\alpha)&=\mathbf{p}_2\mathbf{p}_5I_1\\(X^2-XY\alpha+Y^2\alpha^2)&=\mathbf{p}_2^2\mathbf{p}_{25}I_2\end{aligned}$$

with I_1,I_2 coprime and coprime to 10, and therefore cubes. Writing $(X+Y\alpha)=(\alpha-2)(\alpha-1)\beta^3u^k$ for $u=1-6\alpha+3\alpha^2$ the fundamental unit, $k\in\{0,1,2\}$ and β a generator of I_1. Because $1-6\alpha+3\alpha^2=\frac{(2-\alpha)^3}{2}$, we can rewrite this as

$$\hat{X}+\hat{Y}\alpha=(\alpha-2)(\alpha-1)\hat{\beta}^3$$

where $\hat{X}=2^kX$ and $\hat{Y}=2^kY$ and some $\hat{\beta}$. Let $\hat{\beta}=A+B\alpha+C\alpha^2$, with $3\nmid\mathrm{GCD}(A,B,C)$, else X and Y will not be coprime. Then equate the coefficients of α^2 to obtain

$$0=A^3+6B^3+36C^3+36ABC-9(A^2B+6AC^2+6B^2C)+6(AB^2+A^2C+6BC^2).$$

We easily see $3|A$, from which we get $6B^3\equiv 0 \pmod 9$ so also $3|B$. From this it follows that $36C^3\equiv 0 \pmod{27}$, so $3|C$, giving a contradiction. Thus there are no nontrivial rational solutions to (1.1).

Two Descent

We follow the procedure outlined in [Sil08, Proposition X.1.4] to calculate a 2-descent. There is an action of μ_3 on (1.1) given by $x_i\mapsto\zeta_3^ix_i$, and taking the quotient gives us the elliptic curve

$$E:y^2=x^3+30^2. \tag{1.8}$$

Any rational point on (1.1) also gives a rational point on E. The torsion group is $E(\mathbb{Q})_{\text{tors}}=\{\mathcal{O},(0,30),(0,-30)\}$, and no rational points on (1.1) correspond to these points. If we can show that $E/\mathbb{Q}$ has rank 0, then we will have shown that (1.1) has no rational points.

Let $K=\mathbb{Q}(\zeta_3,\beta)$ where $\beta^3=30$. The class number of K is 9. Then E is given by

$$E:y^2=(x+\beta^2)(x+\zeta_3\beta^2)(x+\zeta_3^2\beta^2). \tag{1.9}$$

Let S be the set of places of K lying over the bad primes of E, which are $\{2,3,5\}$, and let

$$K(S,2)=\{b\in K^\times/(K^\times)^2 \mid \mathrm{ord}_v(b)\equiv 0 \pmod 2 \text{ for all } v\notin S\}.$$

Then we have an injective homomorphism

$$E(K)/2E(K) \longrightarrow K(S,2) \times K(S,2)$$

given by

$$\psi : P = (x,y) \longmapsto \begin{cases} (x+\beta^2, x+\zeta_3\beta^2) & \text{if } x \neq -\beta^2, -\zeta_3\beta^2 \\ \left(\zeta_3+1, \beta^2(\zeta_3-1)\right) & \text{if } x = -\beta^2 \\ \left(\beta^2(1-\zeta_3), -\zeta_3\right) & \text{if } x = -\zeta_3\beta^2 \\ (1,1) & \text{if } P = \mathscr{O}. \end{cases}$$

Let $(b_1,b_2) \in K(S,2) \times K(S,2)$ be a pair that is not the image of one of the three points $\mathscr{O}, (-\beta^2,0), (-\zeta_3\beta^2,0)$. Then (b_1,b_2) is the image of a point

$$P = (x,y) \in E(K)/2E(K)$$

if and only if the equations

$$\begin{aligned} b_1 z_1^2 - b_2 z_2^2 &= \beta^2(1-\zeta_3) \\ b_1 z_1^2 - b_1 b_2 z_3^2 &= \beta^2(1-\zeta_3^2) \end{aligned} \tag{1.10}$$

have a solution $(z_1,z_2,z_3) \in K^\times \times K^\times \times K$. The torsion group $E(K)_{\text{tors}}$ is generated by the two points

$$\begin{aligned} S &= \left((\zeta_3+1)\beta^2, 0\right) \\ T &= \left(2\zeta_3\beta^2, 90\right) \end{aligned}$$

and the only torsion points over $\mathbb{Q}$ are $(0, \pm 30)$. By considering all possible pairs (b_1,b_2), of which there are a finite number and checking local solubility of the system (1.10), we find that the image of ψ is generated by only the two points $\langle \psi(S), \psi(T) \rangle$. Thus there are no nontorsion points of E over K, and by extension there are no nontorsion points of E over $\mathbb{Q}$. Thus $E(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$.

Cassels-Tate Pairing

The third method is the one we shall be employing in this thesis, therefore we give only a brief summary of the result here. Let E be the elliptic curve given in (1.8). Let $\phi : E \to \hat{E}$ be a 3-isogeny with kernel generated by $(0,30)$, and $\hat{\phi} : \hat{E} \to E$ its dual. Descent by 3-isogeny yields

$$\begin{aligned} S^{(\phi)}(E/\mathbb{Q}) &= \langle 1 \rangle \subset \mathbb{Q}(\zeta_3)^\times / (\mathbb{Q}(\zeta_3)^\times)^3 \\ S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) &= \langle 2,3,5 \rangle \subset \mathbb{Q}^\times / (\mathbb{Q}^\times)^3. \end{aligned}$$

The element $30 \in S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ corresponds to the torsion point $(0,30)$. Computing the Cassels-Tate pairing on $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) \times S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) \to \mathbb{Z}/3\mathbb{Z}$ gives us the following matrix.

	2	3	5
2	0	2	1
3	1	0	1
5	2	2	0

This matrix has rank 2. Thus we have two nontrivial elements of $Ш(\hat{E}/\mathbb{Q})[\hat{\phi}]$, and the rank of E is 0. This is precisely the calculation carried out by Cassels in [Cas59] on a slightly different curve.

1.2 Notation

This section contains a summary of the notation used throughout this thesis.

We let K denote a number field, and $\overline{K}$ its algebraic closure. The ring of integers of K will be denoted by O_K. We will use L and M to denote extensions of K, not necessarily Galois. F will be used to denote an arbitrary infinite field. We let $\mu_n \subset \overline{K}$ denote the nth roots of unity, generated by ζ_n, a primitive nth root of unity. We let the places of K be denoted by M_K. For v a place of K, we have K_v the completion of K in the v-adic topology. We let $G_K = \mathrm{Gal}(\overline{K}/K)$, the absolute Galois group of K and $G_{L/K} = \mathrm{Gal}(L/K)$. We also let $H^1(K,-) = H^1(G_K,-)$ to simplify notation.

We will denote an elliptic curve by E/K, being a smooth projective curve of genus 1 with a specified rational point $\mathcal{O} \in E(K)$ which functions as the identity of the group law. Let E_{tors} denote the torsion subgroup of E. For $\phi : E \to \hat{E}$ an isogeny of degree n we let $E[\phi]$ denote its kernel, $\hat{\phi}$ its dual, and $\hat{E}$ is the elliptic curve isogenous to E. We write $[n] : E \to E$ for the multiplication-by-n map. We let $e_n : E[n] \times E[n] \to \mu_n$ be the Weil pairing as defined in [Sil08, III.8]. We also have $e_\phi : E[\phi] \times \hat{E}[\hat{\phi}] \to \mu_n$, the Weil pairing as defined in [Sil08, Exercise 3.15] or Section 3.1.

Let $\#S$ denote the cardinality of a set S. For A any abelian group, we let $A[n]$ denote the n-torsion. For elements $a_0, a_1, a_2, \ldots \in A$, we denote by $\langle a_0, a_1, a_2, \ldots \rangle$ the subgroup of A generated by these elements. For a ring R, we let $R^\times$ denote the group of invertible elements under multiplication. The empty set is given by $\emptyset$, and the trivial group will be denoted either by 0 or by $\langle 1 \rangle$.

If D is a division algebra over a field F, we denote by $M_n(D)$ the ring of $n \times n$ matrices over D. The identity matrix is denoted by I_n. The general linear group, special linear group and projective linear group over F are denoted by $\mathrm{GL}_n(F)$, $\mathrm{SL}_n(F)$ and $\mathrm{PGL}_n(F)$, as usual.

Chapter 2

Descent

Let K be a number field, and E/K an elliptic curve. In this chapter, we will present a few of the basic facts about elliptic curves as well as the descent procedure.

2.1 The Mordell-Weil Theorem

In this section we follow mostly [Sil08]. The most famous theorem concerning elliptic curves is surely the Mordell-Weil theorem.

Theorem 2.1.1 (Mordell-Weil Theorem)**.** *Let E be an elliptic curve and K a number field. Then the group $E(K)$ is finitely generated.*

The Mordell-Weil theorem tells us that the *Mordell-Weil group* $E(K)$ is of the following form

$$E(K) \cong E(K)_{\text{tors}} \times \mathbb{Z}^{r_E}$$

where the torsion subgroup $E(K)_{\text{tors}}$ is finite and the nonnegative integer r_E is called the *rank* of E. In this chapter we set out the basic theoretical underpinnings that has been put in place to try and compute r_E.

The torsion group is easily computed. In fact, Merel ([Mer96]) showed that for any given number field, there are only a finite number of possible torsion groups.

Theorem 2.1.2 (Merel)**.** *For every integer $d \geq 1$ there is a constant $N(d)$ such that for all number fields $K/\mathbb{Q}$ of degree at most d and all elliptic curves E/K we have*

$$|E_{\text{tors}}(K)| \leq N(d).$$

In the case $K = \mathbb{Q}$, we have a theorem by Mazur giving us all the possible torsion groups.

Theorem 2.1.3 (Mazur)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ of $E(\mathbb{Q})$ is isomorphic to one of the following fifteen groups:*

$$\mathbb{Z}/N\mathbb{Z} \text{ with } 1 \leq N \leq 10 \text{ or } N = 12,$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ with } 1 \leq N \leq 4$$

Further, each of these groups occurs as the torsion group for some elliptic curve $E/\mathbb{Q}$.

The Mordell-Weil theorem is proved in two steps, namely a height argument and the weak Mordell-Weil theorem.

Theorem 2.1.4 (Weak Mordell-Weil Theorem)**.** *Let $m \geq 2$ be an integer. Then*

$$E(K)/mE(K)$$

is a finite group.

The Mordell-Weil theorem is now proved using the following descent theorem.

Theorem 2.1.5 (Descent Theorem [Sil08])**.** *Let A be an abelian group. Suppose that there exists a (height) function*

$$h : A \to \mathbb{R}$$

with the three properties

1. *Let $Q \in A$. Then there is a constant c_1 depending on A and Q such that $h(P+Q) \leq 2h(P) + c_1$*
2. *There are an integer $m \geq 2$ and a constant c_2 depending on A such that $h([m]P) \geq m^2 h(P) - c_2$ for all $P \in A$.*
3. *For all constants c_3, the set $\{P \in A \mid h(P) \leq c_3\}$ is finite.*

Suppose further that for the integer m in part 2, the quotient group A/mA is finite. Then A is finitely generated.

The Mordell-Weil theorem is proved by choosing any suitable height function and applying the descent theorem. Thus we see that if we want to compute generators for $E(K)$, we need instead only compute generators for $E(K)/mE(K)$.

2.2 A Geometric Interpretation of the Cohomology Groups

In this section, we review the well-known theory of descent by p-isogeny and give a geometric interpretation of the various cohomology groups we encounter. We follow [Sil08], but other references are available as what follows is very well known. As we saw in the previous section, we are interested in calculating generators for the nontorsion part of $E(K)$. In fact, we actually constrain ourselves to a more modest goal in this thesis, namely bounding, or if possible finding, the number of such generators. This section sets up the method by which this may be done.

We saw in the previous section that it is sufficient to find generators for the finite group $E(K)/mE(K)$ for any integer $m \geq 2$. It is therefore natural to consider the multiplication-by-m map $[m]$, which is an example of an isogeny of degree m^2.

Definition 2.2.1. Let E_1 and E_2 be elliptic curves. An *isogeny* from E_1 to E_2 is a morphism

$$\phi : E_1 \to E_2$$

defined over K satisfying $\phi(\mathcal{O}) = \mathcal{O}$. Two elliptic curves are *isogenous* if there is an isogeny from E_1 to E_2 with $\phi(E_1) \neq \{\mathcal{O}\}$.

From [Sil08, Theorem II.2.3] we know that such a morphism must be surjective on $\overline{K}$-points. We obtain from ϕ the injection of function fields

$$\phi^* : \overline{K}(E_2) \to \overline{K}(E_1)$$

and the degree of ϕ is the degree of the finite extension $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$. For any isogeny $\phi : E \to \hat{E}$ of degree m, there is some isogeny $\hat{\phi} : \hat{E} \to E$, called the *dual isogeny* to ϕ, such that $\hat{\phi} \circ \phi = [m]$. It is often easier to compute $\hat{E}(K)/\phi(E(K))$ and $E(K)/\hat{\phi}(\hat{E}(K))$ than it is to compute $E(K)/mE(K)$, and in fact we still obtain the information we want. For by [Sil08, X.4.7], if ϕ is defined over K there exists the elementary exact sequence

$$0 \to E(K)[\phi] \to E(K)[m] \to \hat{E}(K)[\hat{\phi}] \to \frac{\hat{E}(K)}{\phi(E(K))} \xrightarrow{\hat{\phi}} \frac{E(K)}{mE(K)} \to \frac{E(K)}{\hat{\phi}(\hat{E}(K))} \to 0. \tag{2.1}$$

Thus knowing the other groups in this sequence allows us to compute generators for $E(K)/mE(K)$. To find out more about $\hat{E}(K)/\phi(E(K))$ we find a short exact sequence containing it.

For any nonzero isogeny $\phi : E \to \hat{E}$ defined over K we have an exact sequence of G_K-modules

$$0 \to E[\phi] \to E \xrightarrow{\phi} \hat{E} \to 0. \tag{2.2}$$

By taking Galois cohomology, we obtain the following long exact sequence

$$0 \to E(K)[\phi] \to E(K) \xrightarrow{\phi} \hat{E}(K) \xrightarrow{\delta} H^1(K, E[\phi]) \to H^1(K, E) \xrightarrow{\phi} H^1(K, \hat{E}) \tag{2.3}$$

and from this we obtain the fundamental short exact sequence

$$0 \to \hat{E}(K)/\phi(E(K)) \xrightarrow{\delta} H^1(K, E[\phi]) \to H^1(K, E)[\phi] \to 0. \tag{2.4}$$

The group we are interested in appears here as the first term. To understand it, we must understand the rest of this short exact sequence.

The last group $H^1(K, E)[\phi]$ is the easiest to understand, and we give a geometric interpretation. Every element in $H^1(K, E)$ can be understood as a certain twist of E called a *torsor*.

Definition 2.2.2. Let E/K be an elliptic curve. A *torsor* for E is a pair (T, μ) where T/K is a smooth curve and

$$\mu : T \times E \to T$$

is a simple transitive algebraic group action of E on T.

Two torsors T_1 and T_2 are *equivalent* if there is an isomorphism $\theta : T_1 \to T_2$ defined over K that is compatible with the action of E on T_1 and T_2. The collection of equivalence classes of torsors for E/K is called the *Weil-Chatelet group* for E/K and is denoted by $WC(E/K)$. A torsor T is in the trivial class if and only if $T(K) \neq \emptyset$. Any torsor T is in fact a twist of E.

Definition 2.2.3. Let C/K be a smooth projective curve. A *twist* of C/K is a smooth curve C'/K that is isomorphic to C over $\overline{K}$.

Let (T, μ) be a torsor for E. Fix $P_0 \in T$ and let $\theta : E \to T$, with $\theta(P) = P_0 + P$. We want to show that θ is in fact an isomorphism over $\overline{K}$. For any $\sigma \in G_{\overline{K}/K}$ with $P_0^\sigma = P_0$, we have

$$\theta(P)^\sigma = (P_0 + P)^\sigma = P_0^\sigma + P^\sigma = P_0 + P^\sigma = \theta(P^\sigma)$$

and so θ is defined over $K(P_0)$, and $\deg(\theta) = 1$ by the simple transitivity of the action. Thus by [Sil08, Corollary II.2.4.1], θ is an isomorphism as required.

Therefore there is an isomorphism $\theta^{-1} : T \to E$ defined over $\overline{K}$ such that the cocycle $\sigma(\theta^{-1})\theta$ is an element of the translation subgroup of $\mathrm{Aut}(E)$, the automorphisms of E. The bijection between $WC(E/K)$ and $H^1(K,E)$ can be explicitly given as

$$\{T/K\} \mapsto \{\sigma \mapsto P_0^\sigma - P_0\}$$

where the braces indicate the equivalence class and cohomology class respectively. The trivial class of torsors is thus identified with translation by $\mathscr{O}$. Thus the third group of (2.4) is the ϕ-torsion of $WC(E/K)$.

The second group of (2.4) can also be interpreted geometrically, which we do along the lines of [CFO+08]. We will show that the elements of $H^1(K,E[\phi])$ can be seen as certain twists of E with additional data.

Definition 2.2.4. Let $\phi : E \to \hat{E}$ be an isogeny of elliptic curves, defined over K, and $\hat{\phi} : \hat{E} \to E$ its dual.

1. A *covering* of $\hat{E}$ is a pair (C,π) where C is a smooth projective curve and $\pi : C \to \hat{E}$ is a non-constant morphism.
2. An isomorphism of coverings $(C_1,\pi_1) \cong (C_2,\pi_2)$ is an isomorphism of curves $\theta : C_1 \xrightarrow{\cong} C_2$ with $\pi_1 = \pi_2 \circ \theta$.
3. A ϕ-covering (C,π) is a twist of (E,ϕ).

The ϕ-coverings (C,π) of $\hat{E}$ can be identified with $H^1(K,E[\phi])$ up to isomorphism in the same way as before. Let $\tau : (C,\pi) \xrightarrow{\cong} (E,\phi)$ be defined over $\overline{K}$. We associate to (C,π) the cocycle $\sigma(\tau)\tau^{-1}$, which is an element of $H^1(K,\mathrm{Aut}(E,\phi))$. Let $\theta : E \to E$ be an automorphism of (E,ϕ). Then $\phi = \phi \circ \theta$ and so $\phi \circ (\theta - 1) = 0$. Therefore $\theta - 1$ is a nonsurjective morphism, which means it must be constant by [Sil08, II.2.3]. Therefore θ must be translation by a ϕ-torsion point and we have associated to (C,π) an element of $H^1(K,E[\phi])$ obtaining a bijection

$$\{(C,\pi)\}/\cong \longleftrightarrow H^1(K,E[\phi]).$$

From this point onwards, assume that $[K:\mathbb{Q}] < \infty$. Now that we have a geometric interpretation for both the cohomology groups appearing in (2.4), we want to replace them with certain finite groups. This is done by considering the local version for each $v \in M_K$. For each such v, we fix an embedding $\overline{K} \subset \overline{K}_v$ and a decomposition group $G_v \subset G_K$. Following the same construction as before, we obtain the short exact sequence

$$0 \to \hat{E}(K_v)/\phi(E(K_v)) \xrightarrow{\delta_v} H^1(K_v,E[\phi]) \to H^1(K_v,E)[\phi] \to 0 \tag{2.5}$$

for every place $v \in M_K$. Replacing the third group by the Weil-Chatelet group, we are naturally led to consider the following large commutative diagram.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \hat{E}(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(K,E[\phi]) & \xrightarrow{\gamma} & WC(E/K)[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_{v\in M_K} \hat{E}(K_v)/\phi(E(K_v)) & \xrightarrow{\{\delta_v\}} & \prod_{v\in M_K} H^1(K_v,E[\phi]) & \xrightarrow{\{\gamma_v\}} & \prod_{v\in M_K} WC(E/K_v)[\phi] & \longrightarrow & 0
\end{array}$$

Seeing as we are interested in knowing the size of $\hat{E}(K)/\phi(E(K))$, this means we would like to compute the image of the map δ or, equivalently, the kernel of the map γ. Computing $\ker(\gamma)$ comes down to calculating whether certain torsors of E have a K-rational point, which is usually a difficult problem. However, computing $\ker(\gamma_v)$ for each v is much easier. For by Hensel's lemma, if a curve has a point over some finite ring O_{K_v}/M_v^e, for some easily computable integer e and M_v a maximal ideal, then it can be lifted to a point over K_v. This is therefore a finite computation. These considerations prompt the following definitions.

Definition 2.2.5. Let $\phi : E/K \to \hat{E}/K$ be an isogeny. The ϕ-Selmer group of E/K is the subgroup of $H^1(K, E[\phi])$ defined by

$$S^{(\phi)}(E/K) = \ker \left\{ H^1(K, E[\phi]) \to \prod_{v \in M_K} WC(E/K_v) \right\}.$$

The Shafarevich-Tate group of E/K is the subgroup of $WC(E/K)$ defined by

$$Ш(E/K) = \ker \left\{ WC(E/K) \to \prod_{v \in M_K} WC(E/K_v) \right\}.$$

Thus the Selmer group $S^{(\phi)}(E/K)$ consists of the ϕ-coverings of $\hat{E}$ that have points everywhere locally, and the Shafarevich-Tate group $Ш(E/K)$ corresponds to the group of torsors under E that have points everywhere locally. These groups form a short exact sequence.

$$0 \to \hat{E}(K)/\phi(E(K)) \xrightarrow{\delta_\phi} S^{(\phi)}(E/K) \to Ш(E/K)[\phi] \to 0. \tag{2.6}$$

Computing the Selmer group $S^{(\phi)}(E/K)$ is referred to as calculating a ϕ-descent or, if $\deg(\phi) = p$, doing a descent by p-isogeny. It is well known that Selmer groups are finite [Sil08, Theorem X.4.2] and we will see in Section 2.7 exactly how they are used in rank estimates.

2.3 Interpreting the First Cohomology Groups Using Étale Algebras

In this section, let $\phi : E \to \hat{E}$ be an isogeny of degree p, where p is a prime. Let $\hat{\phi} : \hat{E} \to E$ be its dual. Previously, we interpreted the Selmer groups $S^{(\phi)}(E/K)$ and $S^{(p)}(E/K)$ as geometric objects. In this section, we express them as subquotients of the unit groups of certain étale algebras, as is done in [SS03]. We have $S^{(\phi)}(E/K) \subset H^1(K, E[\phi])$ and $S^{(p)}(E/K) \subset H^1(K, E[p])$, so these are the cohomology groups we are interested in. In fact, in this section we can work with any infinite field F rather than just the number field K.

Definition 2.3.1. An *étale algebra* D over any infinite field F is the finite product

$$D \cong D_1 \times \ldots \times D_n$$

where D_i is a finite separable field extension of F for each i.

Let $\overline{D} = D \otimes_F \overline{F}$ where $\overline{F}$ is a separable closure of F.

From the Kummer sequence

$$0 \to \mu_p(\overline{D}) \to \overline{D}^\times \xrightarrow{[p]} \overline{D}^\times \to 0 \tag{2.7}$$

we obtain the following long exact sequence.

$$0 \to \mu_p(\overline{D}) \to \overline{D}^\times \xrightarrow{[p]} \overline{D}^\times \to H^1(F, \mu_p(\overline{D})) \to H^1(F, \overline{D}^\times). \tag{2.8}$$

By a generalisation of Hilbert's theorem 90, we know that $H^1(F, \overline{D}^\times) = 0$. Thus we obtain the Kummer isomorphism

$$\kappa : H^1(F, \mu_p(\overline{D})) \xrightarrow{\cong} D^\times/(D^\times)^p. \tag{2.9}$$

More abstractly, an étale algebra D corresponds to a finite étale scheme X over F. We can therefore interpret $\overline{D}$ as the functions from points $X(\overline{F})$ into $\overline{F}$. Similarly, D corresponds to the subset of Galois-invariant functions, $D^\times$ the Galois-invariant functions into $\overline{F}^\times$, and $\mu_p(\overline{D})$ the functions into μ_p.

Let ψ denote either the p-isogeny ϕ or the multiplication-by-p map $[p]$, with $\hat{\psi}$ its dual. Let X denote a Galois-invariant subset of $\hat{E}[\hat{\psi}] \setminus \{\mathscr{O}\}$ that generates $\hat{E}[\hat{\psi}]$, and D the étale algebra corresponding to X. Let

$$\begin{aligned} w_\psi : E[\psi] &\to \mu_p(\overline{D}) \\ R &\mapsto (P \mapsto e_\psi(R,P)) \end{aligned} \tag{2.10}$$

where e_ψ is the Weil pairing, defined in Section 3.1 for the p-isogeny case and in [Sil08, Section III.8] in the multiplication-by-p case. Because X spans $\hat{E}[\hat{\psi}]$, and e_ψ is nondegenerate and bilinear, w_ψ is injective. We now define the induced map

$$\overline{w}_\psi : H^1(F, E[\psi]) \to H^1(F, \mu_p(\overline{D})). \tag{2.11}$$

By applying $\kappa \circ \overline{w}_\psi$ to $H^1(F,E[\psi])$, we thus obtain a group homomorphism of $H^1(F,E[\psi])$ into $D^\times/(D^\times)^p$. Of course, for this course of action to be successful in giving a concrete description of $H^1(F,E[\psi])$, we must show that $\overline{w}_\psi$ is injective, and then find its image. There are two cases we are interested in in this thesis.

1. Let ψ denote some p-isogeny ϕ, so $X = E[\phi] \setminus \{\mathscr{O}\}$ and we consider $H^1(F,E[\phi])$.
2. Let ψ be the multiplication-by-p map, so $X = E[p] \setminus \{\mathscr{O}\}$ and we consider $H^1(F,E[p])$.

The Case ψ is a p-isogeny

This first case is much simpler than the second. Let $\phi : E \to \hat{E}$ be a p-isogeny and $\hat{\phi} : \hat{E} \to E$ its dual. Let A_2 and A_1 denote the étale F-algebras corresponding to $E[\phi] \setminus \{\mathscr{O}\}$ and $\hat{E}[\hat{\phi}] \setminus \{\mathscr{O}\}$ respectively. We see that A_1 has degree $p-1$ over F and $\dim(\mu_p(\overline{A}_1))$ is $p-1$. Before proceeding, we need some notation.

Notation 2.3.2. *Let M be a finite dimensional $\mathbb{F}_p$-vector space with linear $GL_2(\mathbb{F}_p)$-action. Then we write $M^{(t)}$ with $t \in \mathbb{Z}/(p-1)\mathbb{Z}$ for the subspace of M on which a matrix αI, with $\alpha \in \mathbb{F}_p^\times$, acts as multiplication by α^t.*

For any such a finite dimensional $\mathbb{F}_p$-vector space M, we have that

$$M = M^{(0)} \oplus M^{(1)} \oplus \cdots \oplus M^{(p-2)}.$$

The map w_ϕ then gives an isomorphism $w_\phi : E[\phi] \xrightarrow{\cong} \mu_p(\overline{A}_1)^{(1)}$. Thus by [SS03, Lemma 5.2], we find

$$H^1(F,E[\phi]) \cong \ker(g - \sigma_g : A_1^\times/(A_1^\times)^p \to A_1^\times/(A_1^\times)^p) \tag{2.12}$$

where g is a primitive root mod p and σ_g is the corresponding automorphism of A_1/F. In the interpretation of an element of $A_1^\times$ as a function χ of $\hat{E}[\hat{\phi}]$, the automorphism σ_g is given by $(\sigma_g\chi)(P) = \chi(g \cdot P)$.

Notation 2.3.3. *Let $L = F(\alpha)$ for some $\alpha \notin F$ such that $\alpha^2 \in F$. Let $G = G_{L/F} = \langle \tau \rangle$. Let $V = L^\times/(L^\times)^p$ for some odd prime p. Then we denote by $V^\pm$ the $\pm$-eigenspace for the action of G on V.*

Example 2.3.4. (i) Assume that $E[\phi] \cong \mu_3$. Then we obtain from the standard Kummer isomorphism (2.9) that $H^1(F,\mu_3) \cong F^\times/(F^\times)^3$.

(ii) Assume that $E[\phi] \cong \mathbb{Z}/3\mathbb{Z}$ and $\zeta_3 \notin F$. Then we have $A_1 \cong L = F(\zeta_3)$. Let $\mathrm{Gal}(L/F) = \langle \tau \rangle$ be the Galois group of L over F. There are two eigenspaces for the action of $\mathrm{Gal}(L/F)$ on $L^\times/(L^\times)^3$, and we find $H^1(F,\mathbb{Z}/3\mathbb{Z}) \cong \left(L^\times/(L^\times)^3\right)^-$.

The Case ψ is the multiplication-by-p Map

We make use of [DSS00]. Let A be the étale algebra corresponding to $X = E[p] \setminus \{\mathscr{O}\}$. Recall the interpretation of A as maps from X to $\overline{F}$, and extend all maps to let $\mathscr{O} \mapsto 1$. Thus we obtain

$$\overline{A}^\times = \{\varepsilon : E[p] \to \overline{F}^\times \mid \varepsilon(\mathscr{O}) = 1\}$$

Let $L = F(E[p])$ and $G = G_{L/F}$. Choosing a basis for $E[p]$, we can view G as a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

Proposition 2.3.5. *$\overline{w}_p$ is injective.*

Proof. By Section 3 of [DSS00], the problem is reduced to showing that its restriction

$$\overline{w}_p : H^1(G, E[p]) \to H^1(G, \mu_p(\overline{A}))$$

is injective. Thus if $p \nmid \#G$ then we see quickly that $\overline{w}_p$ is injective. For since the orders of G and $E[p]$ are then coprime, we have $H^1(G, E[p]) = 0$.

If $p \mid \#G$, then Lemmas 4, 5 and 6 of [DSS00] show that $\overline{w}_p$ is injective. □

We are now interested in finding the image of $\kappa \circ \overline{w}_p$. First we need some more definitions. Let A_+ denote the étale subalgebra of A corresponding to the orbits in $E[p] \setminus \{\mathscr{O}\}$ of $Z = \mathbb{F}_p^\times I$, where I is the identity matrix in $GL_2(\mathbb{F}_p)$. Then A is an extension of degree $p-1$ of A_+, and the automorphism group of A/A_+ is cyclic of order $p-1$.

Let $E[p]^\vee = \mathrm{Hom}(E[p], \mathbb{Z}/p\mathbb{Z})$. Then we identify the set $E[p]^\vee \setminus \{\mathscr{O}\}$ with the affine lines in $E[p]$ missing the origin in the following way.

$$l \longleftrightarrow \varepsilon \Longleftrightarrow l = \{P \in E[p] \mid \varepsilon(P) = 1\}.$$

We let B denote the étale algebra corresponding to this set of affine lines. We have a map u given by

$$\begin{aligned} u : \mu_p(\overline{A}) &\longrightarrow \mu_p(\overline{B}) \\ \varepsilon &\longmapsto \left(l \mapsto \prod_{P \in l} \varepsilon(P) \right) \end{aligned}$$

which induces a map $\overline{u}$

$$A^\times/(A^\times)^p = H^1(F, \mu_p(\overline{A})) \xrightarrow{\overline{u}} H^1(F, \mu_p(\overline{B})) = B^\times/(B^\times)^p.$$

Making $\overline{u}$ explicit, we need to define D as the étale algebra corresponding to the set of all pairs $(P, l) \in (E[p] \setminus \{\mathscr{O}\}) \times (E[p]^\vee \setminus \{\mathscr{O}\})$ such that $P \in l$. Then it can be shown that $\overline{u}$ is induced by the composition $N_{D/B} \circ i_{D/A} : A \to B$ where $i_{D/A}$ is the inclusion $A \to D$ and $N_{D/B}$ the norm from D to B.

The following corollary follows from [SS03, Proposition 5.8] and gives a complete characterisation of $H^1(F, E[p])$.

Corollary 2.3.6. *[SS03] We have*

$$H^1(F, E[p]) \cong \ker(g - \sigma_g : A^\times/(A^\times)^p \to A^\times/(A^\times)^p) \cap \ker(\overline{u})$$

where $\overline{u}$ is the map induced by u on H^1, and g is a primitive root mod p, with σ_g the corresponding automorphism of A/A_+.

As before, we interpret the elements of $A^\times$ as functions χ on $E[p]$, and the automorphism σ_g is given by $(\sigma_g \chi)(P) = \chi(g \cdot P)$.

2.4 Descent by 3-Isogeny

In this section, we follow mainly [Top91]. To compute a descent by p-isogeny for $p > 3$, we refer to [MS13].

To admit an isogeny ϕ of degree 3, the elliptic curve E must have some point S of order 3 defined over $\overline{K}$ with $g_S = \langle S \rangle$, stable under the action of $G_{K_s/K}$, to serve as a generator of the kernel of ϕ. We can give E/K by a Weierstrass equation $y^2 = f(x)$, with f a degree 3 polynomial. In this case, g_S will be $\{O, S, -S\}$ where $S = (\alpha, \beta)$ and $-S = (\alpha, -\beta)$. The Galois invariance implies that $\alpha \in K$ and $\beta^2 \in K$. We can now do a change of coordinates to send $\alpha \mapsto 0$. By using the duplication formula and setting $2T = -T$ we obtain an equation for E of the form

$$E : y^2 = x^3 + Ax^2 + Bx + C$$

where $B^2 = 4AC$. Thus we obtain for E an equation of the form

$$E : y^2 = x^3 + \Delta(\varepsilon x + \eta)^2$$

for integers ε, η and Δ. The isogenous curve is obtained by dividing out by the subgroup g_S. We obtain [CP09]

$$\hat{E} : x^3 + \hat{\Delta}(\hat{\varepsilon} x + \hat{\eta})^2$$

where $\hat{\Delta} = -3\Delta$, $\hat{\varepsilon} = \varepsilon$ and $\hat{\eta} = \frac{27\eta - 4\varepsilon^3\Delta}{9}$. The isogeny ϕ is given by

$$\phi(P) = \left(\frac{x^3 + 4\Delta((\varepsilon^2/3)x^2 + \varepsilon\eta x + \eta^2)}{x^2}, \frac{y(x^3 - 4\Delta\eta(\varepsilon x + 2\eta))}{x^3} \right).$$

The points of order 3 on E are generated by $S = (0, \eta\sqrt{\Delta})$ and $T = (\beta, \frac{\sqrt{\Delta}(\varepsilon\beta + 3\eta)}{\sqrt{-3}})$, where β is a root of the cubic $\psi(x) = 3x^3 + 4\varepsilon^2\Delta x^2 + 12\varepsilon\eta\Delta x + 12\eta^2\Delta$. The kernel of ϕ is generated by S.

Recall that we have interpreted the elements of $S^{(\phi)}(E/K)$ to be the isomorphism classes of ϕ-coverings of $\hat{E}$ that have points everywhere locally. From [CP09] we obtain the following equations for these ϕ-coverings. If $\Delta = 1$, an element of $S^{(\phi)}(E/K)$ can be represented by some $u \in K^\times/(K^\times)^3$ or by the ϕ-covering

$$C_u : uX^3 + \frac{1}{u}Y^3 + 2\eta Z^3 - 2\varepsilon XYZ = 0. \tag{2.13}$$

If $\Delta \neq 1$, then by equation (2.12) with $g = -1$ an element of $S^{(\phi)}(E/K)$ can be represented by some $u \in (K(\sqrt{\Delta})^\times/(K(\sqrt{\Delta})^\times)^3)^-$ (see Definition 2.3.3), so $N_{K(\sqrt{\Delta})/K}(u) \in (K^\times)^3$. Let $\mathrm{Gal}(K(\sqrt{\Delta})/K) = \langle \tau \rangle$. With $v = v_1 + v_2\sqrt{\Delta}$, we substitute the following into (2.13).

$$\begin{aligned} u &= v^2\tau(v) \\ \varepsilon &= \varepsilon\sqrt{\Delta} \\ \eta &= \eta\sqrt{\Delta}. \end{aligned}$$

Let $Y = -\frac{1}{v\tau(v)}Y$ to obtain

$$C'_v : 2\varepsilon\sqrt{\Delta}XYZ + vX^3 - \tau(v)Y^3 + \frac{2\eta\sqrt{\Delta}}{v\tau(v)}Z^3 = 0. \tag{2.14}$$

Via the change of coordinates

$$\begin{aligned} X &\to X - \sqrt{\Delta}Y \\ Y &\to X + \sqrt{\Delta}Y \\ Z &\to Z \end{aligned}$$

we obtain

$$C_v : 2v_2X^3 + 2\Delta v_1Y^3 + \frac{2\eta}{v_1^2 - \Delta v_2^2}Z^3 + 6v_1X^2Y + 6v_2\Delta XY^2 + 2\varepsilon(X^2Z - \Delta Y^2Z) = 0. \tag{2.15}$$

Finding a K-rational point on C_v is equivalent to finding a $K(\sqrt{\Delta})$-rational point on C'_v. Thus an element $u \in \left(K(\sqrt{\Delta})^\times/(K(\sqrt{\Delta})^\times)^3\right)^-$ is an element of $S^{(\phi)}(E/K)$ if and only if C_v is everywhere locally soluble. To compute a descent by 3-isogeny, we can find in [Top91] or [CP09] a finite set in $\left(K(\sqrt{\Delta})^\times/(K(\sqrt{\Delta})^\times)^3\right)^-$ in which all Selmer elements must lie. By checking local solubility for each candidate, we can then determine the Selmer group.

2.5 Diagrams for the 3-Isogeny Case

We focus again on the 3-isogeny case. The action of G_K on $E[3]$ factors through a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. It is known that $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ has 16 subgroups up to conjugacy, only 8 of which can occur when $K = \mathbb{Q}$. Excepting for C_8, all other subgroups of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ are contained in $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ and thus do not occur because $\zeta_3 \notin \mathbb{Q}$. If we have $\mathrm{Gal}(E[3]) \cong C_8$, then the degree 4 subfield of $\mathbb{Q}(E[3])$ must be totally real, which is impossible since $\zeta_3 \in \mathbb{Q}(E[3])$. The 8 occurring subgroups are labelled as in the MAGMA function `ThreeTorsionType`. The table below gives generators for G in each case.

label	generators for G	order
`Generic`	$\begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}2&1\\1&0\end{pmatrix}$	48
`2Sylow`	$\begin{pmatrix}1&0\\2&2\end{pmatrix}, \begin{pmatrix}0&2\\1&0\end{pmatrix}$	16
`Generic3Isogeny`	$\begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}2&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	12
`dihedral`	$\begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}0&2\\1&0\end{pmatrix}$	8
`Z/3Z-nonsplit`	$\begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	6
`mu3-nonsplit`	$\begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	6
`Diagonal`	$\begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}$	4
`mu3+Z/3Z`	$\begin{pmatrix}1&0\\0&2\end{pmatrix}$	2

We will concentrate on just a few of these. The Cassels-Tate pairing for curves of type $\mu_3 + \mathbb{Z}/3\mathbb{Z}$ was calculated in [Fis03], and we refer to Section 2.6.2 for a brief overview. In this thesis we encounter mostly curves of type $\mathbb{Z}/3\mathbb{Z}$-nonsplit and μ_3-nonsplit. In this section, we give some important diagrams and theorems for use in examples later.

In this section, we shall frequently encounter the second cohomology group. To understand these groups, we introduce the Brauer group, first introduced by R. Brauer in [Bra28, Bra30], for which we give the references [NSW08, GS06]. This is a group dealing with *central simple algebras*, that is, finite dimensional K-algebras with centre K and without nontrivial two-sided ideals. We say a central simple K-algebra A *splits* over an extension L/K if $A \otimes_K L \cong M_n(L)$ for some n. There are many good background references for such algebras, such as [BO13].

Example 2.5.1. A special case of a central simple algebra is a *cyclic algebra*. Let L/K be a cyclic Galois extension of degree m with Galois group $G_{L/K} = G$. Let $\chi : G \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z}$, a character of G, and let σ be such that $\chi(\sigma) = 1$. Then for any $a \in K^\times$ we can define the K-algebra

$$(\chi, a) = \bigoplus_{i=0}^{m-1} e^i L$$

generated by the single element e subject to the relations

$$\begin{aligned} e^m &= a \\ \lambda e &= e\lambda^\sigma \text{ for all } \lambda \in L. \end{aligned}$$

The algebra (χ, a) is known as a cyclic algebra.

Definition 2.5.2. Two central simple K-algebras A and A' are called *Brauer equivalent* if $A \otimes_K M_m(K) \cong A' \otimes_K M_{m'}(K)$ for some $m, m' > 0$.

Thus we are led to consider the following definition.

Definition 2.5.3. The *Brauer group* $\mathrm{Br}(K)$ of a field K is the set of all Brauer equivalent classes $[A]$ of central simple K-algebras A, endowed with the multiplication

$$[A] \cdot [B] = [A \otimes_K B].$$

We can also define the *Brauer group* $Br(L/K)$ *of* K *relative to* L for some finite Galois extension L/K as the kernel of the restriction homomorphism

$$\begin{aligned} \mathrm{res}^K_L : \mathrm{Br}(K) &\longrightarrow \mathrm{Br}(L) \\ A &\longmapsto [A \otimes_K L]. \end{aligned}$$

If we let L/K run through all finite Galois extensions of K, then we have

$$\mathrm{Br}(K) = \bigcup_L \mathrm{Br}(L/K).$$

In fact, it needs to be proved that $\mathrm{Br}(L/K)$ and $\mathrm{Br}(K)$ are groups at all, which is done in [GS06, Proposition 2.4.8]. The following theorem makes the connection between Brauer groups and the second cohomology group.

Theorem 2.5.4 ([GS06, Theorem 4.4.7]). *Let K be a field, L/K a finite Galois extension and K_s a separable closure of K. Let G be the Galois group $G_{L/K}$. There exist natural isomorphisms of abelian groups*

$$\mathrm{Br}(L/K) \cong H^2(G, L^\times)$$

and

$$\mathrm{Br}(K) \cong H^2(K, K_s^\times).$$

If L/K is a Galois extension of degree n, then each element of the relative Brauer group $\mathrm{Br}(L/K)$ has order dividing n. Hence $\mathrm{Br}(K)$ is a torsion abelian group [GS06, Corollary 4.4.8]. The following two corollaries are crucial in understanding our methods in the rest of this chapter.

Corollary 2.5.5 ([GS06, 4.4.9]). *For each positive integer m prime to the characteristic of K we have a canonical isomorphism*

$$\mathrm{Br}(K)[m] \cong H^2(K, \mu_m).$$

(Recall that μ_m denotes the group of mth roots of unity in a separable closure K_s of K equipped with its canonical action.)

Proof. From the Kummer exact sequence

$$1 \longrightarrow \mu_m \longrightarrow K_s^\times \xrightarrow{[m]} K_s^\times \longrightarrow 1$$

we obtain the following section of the associated long exact sequence

$$H^1(K, K_s^\times) \longrightarrow H^2(K, \mu_m) \longrightarrow H^2(K, K_s^\times) \longrightarrow H^2(K, K_s^\times).$$

The first group is trivial by Hilbert's Theorem 90. The last map is multiplication by m, therefore the corollary follows. □

Corollary 2.5.6 ([GS06, 4.4.10]). *For a cyclic Galois extension L/K there is a canonical isomorphism*

$$\mathrm{Br}(L/K) \cong K^\times / N_{L/K}(L^\times).$$

In the following subsections, we explore three of the possible isogeny cases and make certain cohomology groups explicit.

2.5.1 μ_3-nonsplit

When we are in the μ_3-nonsplit case, the action of G_K on $E[3]$ factors through the subgroup G consisting of all matrices of the form

$$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}.$$

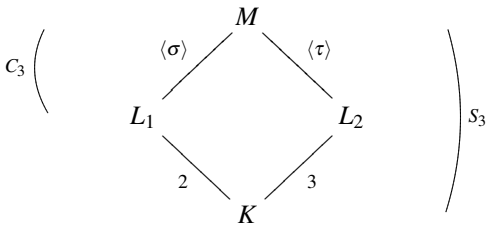
We choose generators $S, T \in E[3]$ and $\sigma, \tau \in G$ such that

$$\begin{aligned} \sigma(S) &= S & \qquad \tau(S) &= 2S \\ \sigma(T) &= S+T & \qquad \tau(T) &= T \end{aligned}$$

thus $\sigma \leftrightarrow \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\tau \leftrightarrow \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Define the following fields

$$\begin{aligned} M &= K(E[3]) \\ L_1 &= K(S) = K(\zeta_3) \\ L_2 &= K(T) \end{aligned}$$

with $[M:K]=6$, $[L_1:K]=2$ and $[L_2:K]=3$. Thus we have the following diagram



where $L_1 = K(\zeta_3)$ and $M = K(\zeta_3, \sqrt[3]{\beta})$ for some $\beta \in L_1$. In fact, because τ is represented by a diagonal (and therefore diagonalizable) matrix, the basis of the space it operates on can be given by eigenvectors. Thus we can find one generator, S, whose coordinates lie in the negative eigenspace and one generator, T, whose coordinates lie in the positive eigenspace of L_1. We can therefore find $\beta \in K$ with $L_2 = K(\sqrt[3]{\beta})$.

Let ϕ be the 3-isogeny whose kernel is generated by S, and ι the inclusion map. From the exact sequence of G_K-modules

$$0 \to E[\phi] \xrightarrow{\iota} E[3] \xrightarrow{\phi} \hat{E}[\hat{\phi}] \to 0$$

we obtain the following long exact sequence by taking Galois cohomology.

$$\mathbb{Z}/3\mathbb{Z} \to H^1(K,E[\phi]) \xrightarrow{\iota_*} H^1(K,E[3]) \xrightarrow{\phi_*} H^1(K,\hat{E}[\hat{\phi}]) \to H^2(K,E[\phi])$$

In this case, we have $E[\phi] \cong \mu_3$ and $\hat{E}[\hat{\phi}] \cong \mathbb{Z}/3\mathbb{Z}$. Recall from Example 2.3.4 that we have $H^1(K,\mu_3) \cong K^\times/(K^\times)^3$ and $H^1(K,\mathbb{Z}/3\mathbb{Z}) \cong (L_1^\times/(L_1^\times)^3)^-$. We have also seen in Corollary 2.5.5 that $H^2(K,\mu_3) \cong \mathrm{Br}(K)[3]$. The following lemma gives an explicit way of expressing the elements of $H^1(K,E[3])$.

Lemma 2.5.7. *The group $H^1(K,E[3])$ is isomorphic to the subgroup H of pairs (a,b) in $L_1^\times/(L_1^\times)^3 \times L_2^\times/(L_2^\times)^3$ satisfying*

$$N_{L_2/K}(b) \in (K^\times)^3 \text{ and } \frac{\sigma(b)}{ab} \in (M^\times)^3.$$

Proof. We must satisfy the conditions of Corollary 2.3.6.

There are 3 orbits for the action of G_K on $E[3]\setminus\{\mathcal{O}\}$, with representatives $S, T, -T$. From Section 2.3, we see that $H^1(K,E[3]) \subset A^\times/(A^\times)^3$ where $A \cong L_1 \times L_2 \times L_2$. Any element in $H^1(K,E[3])$ represented by (a,b,b') will have $b' = b^2 \pmod{}(L_2^\times)^3$, thus we can represent the element as $(a,b) \in L_1^\times/(L_1^\times)^3 \times L_2^\times/(L_2^\times)^3$.

By Corollary 2.3.6, the element (a,b) must lie in $\ker(g-\sigma_g)$, for g some primitive root mod 3, and σ_g the corresponding automorphism of A. Thus in this case, $g=2$. The associated automorphism σ_2 sends $S \mapsto 2S$ and $T \mapsto 2T$. Thus

$$\begin{aligned}(2-\sigma_2)(a,b) &= \left(\frac{a^2}{\tau(a)}, \frac{b^2}{b'}\right) \\ &= \left(\frac{a^2}{\tau(a)}, \frac{b^2}{b^2}\right)\end{aligned}$$

and we find that we must have $N_{L_1/K}(a) \in (K^\times)^3$. This condition follows from the two conditions mentioned in the lemma, because

$$N_{M/L_2}\left(\frac{\sigma(b)}{ab}\right) = \frac{N_{L_2/K}(b)}{N_{L_1/K}(a)b^3} \in (L_2^\times)^3.$$

The second part of Corollary 2.3.6 involves finding the kernel of some map $\overline{u}$, which we make explicit in this case as follows. The set $E[3]^\vee\backslash\{\mathscr{O}\}$ of affine lines in $E[3]$ missing the origin form three orbits under G_K, represented by

$$(T,S+T,-S+T),(-T,S-T,-S-T),(-S,-T,S+T). \tag{2.16}$$

The first two orbits contain just one line each, the third contains six lines, thus the étale algebra corresponding to $E[3]^\vee\backslash\{\mathscr{O}\}$ is $B \cong K\times K\times M$. Let D be the étale algebra corresponding to the set of all pairs $(P,l) \in (E[3]\setminus\{\mathscr{O}\})\times E[3]^\vee\backslash\{\mathscr{O}\}$. Then $\overline{u}(a,b)$ is given by the inclusion of (a,b) into D, followed by the norm from D into B, given by the three representatives given in (2.16). Thus we must have

$$\begin{aligned}(T,S+T,-S+T) &\longleftrightarrow b\sigma(b)\sigma^2(b) \in (K^\times)^3\\ (-T,S-T,-S-T) &\longleftrightarrow b^2\sigma(b)^2\sigma^2(b)^2 \in (K^\times)^3\\ (-S,-T,S+T) &\longleftrightarrow a^2b^2\sigma(b) \in (M^\times)^3\end{aligned}$$

We see that we must therefore have $N_{L_2/K}(b) \in (K^\times)^3$ and $\frac{\sigma(b)}{ab} \in (M^\times)^3$. From Corollary 2.3.6, we see that $H^1(K,E[3])$ consists of the intersection of $\ker(\overline{u})$ with $\ker(2-\sigma_2)$, thus $H^1(K,E[3]) \cong H$, as required. □

Thus we obtain the following diagram.

$$\begin{array}{ccccccccc}
\hat{E}[\hat{\phi}] & \xrightarrow{\Delta_1} & H^1(K,E[\phi]) & \xrightarrow{\iota_*} & H^1(K,E[3]) & \xrightarrow{\phi_*} & H^1(K,\hat{E}[\hat{\phi}]) & \xrightarrow{\Delta_2} & H^2(K,E[\phi]) \\
\downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong \\
\mathbb{Z}/3\mathbb{Z} & \xrightarrow{\delta_1} & K^\times/(K^\times)^3 & \xrightarrow{f} & H & \xrightarrow{g} & (L_1^\times/(L_1^\times)^3)^- & \xrightarrow{\delta_2} & \mathrm{Br}(L_1)^+
\end{array} \tag{2.17}$$

The vertical isomorphisms are all given either by the theory in Section 2.3 or by Lemma 2.5.7. The map δ_1 sends 1 to a Kummer generator for M/L_1. The map δ_2 sends a to the cyclic algebra (χ,a) where $\chi : G_{M/L_1} \cong \frac{1}{3}\mathbb{Z}/\mathbb{Z}$ is the isomorphism fixed by sending $\sigma \mapsto 1$. Any element $a \in S^{(\hat{\phi})}(\hat{E}/K)$, lying in $H^1(K,\mathbb{Z}/3\mathbb{Z})$, necessarily lies in the image of the map ϕ_*. By the explicit description of $\delta_2(a)$ as a cyclic algebra, and Corollary 2.5.6, we see that lifting a to $H^1(K,E[3])$ amounts to solving a norm equation in the cyclic Galois extension M/L_1. This can be a computationally heavy task, and we explore improvements to this calculation for cubic extensions in Chapter 4.

We are left with determining the maps f and g. We claim that

$$\begin{aligned}f &: b \mapsto (1,b)\\ g &: (a,b) \mapsto a.\end{aligned}$$

Of course, we now need to prove that these are the correct choices to make, which is done in the following theorem.

Theorem 2.5.8. *The diagram* (2.17) *is commutative.*

Proof. We have chosen generators S and T for $E[3]$, where $E[\phi] = \langle S\rangle$ and the Weil pairing e_3 gives $e_3(S,T) = \zeta_3$. We also have $K(T) = K(\sqrt[3]{\beta})$ for some $\beta \in K$. Let $\hat{S}$ generate $\hat{E}[\hat{\phi}]$ such that $\phi(T) = \hat{S}$. Let the isomorphism $\hat{\varepsilon} : \hat{E}[\hat{\phi}] \cong \mathbb{Z}/3\mathbb{Z}$ be given by $\hat{S} \mapsto 1$ and the isomorphism $\varepsilon : E[\phi] \cong \mu_3$ by $S \mapsto \zeta_3$. Then $\Delta_1(\hat{S})$ corresponds to the cohomology class in $H^1(K,E[\phi])$ given by the 1-cocycle ξ with

$$\xi_\rho = \rho(T) - T.$$

Under the isomorphism $H^1(K,E[\phi]) \cong H^1(K,\mu_3)$, this becomes the 1-cocycle ξ with

$$\xi_\rho = \frac{\rho(\sqrt[3]{\beta})}{\sqrt[3]{\beta}}.$$

By the Kummer isomorphism, we have

$$\left(\rho \mapsto \frac{\rho(\sqrt[3]{\beta})}{\sqrt[3]{\beta}}\right) \longleftrightarrow \beta \in K^\times/(K^\times)^3.$$

The map δ_1 sends 1 to a Kummer generator for M/L_1, which is precisely the β above, thus the first square commutes.

We prove now that f makes the square it is in commute. Let us consider a cocycle class $\xi \in H^1(K,E[\phi])$. As before, using the isomorphism $\varepsilon : E[\phi] \cong \mu_3$ and the Kummer isomorphism yields

$$(\rho \mapsto \rho(T) - T) \longleftrightarrow \left(\rho \mapsto \frac{\rho(\sqrt[3]{\beta})}{\sqrt[3]{\beta}}\right) \longleftrightarrow \beta \in K^\times/(K^\times)^3.$$

The map f then gives us $(1,\beta) \in H$. We have $N_{L_1/K}(1)$, $N_{L_2/K}(\beta) \in (K^\times)^3$ and $\frac{\sigma(\beta)}{\beta} = \frac{\beta}{\beta} = 1 \in (M^\times)^3$ as required. Following Section 2.3 and using the Weil pairing, we define the map

$$\begin{aligned} E[\phi] \xrightarrow{\iota} E[3] &\xrightarrow{w_3} \mathrm{Maps}(\{\pm S\},\mu_3) \times \mathrm{Maps}(\{T, T\pm S\},\mu_3) = \mu_3(\overline{L}_1) \times \mu_3(\overline{L}_2) \\ S \longmapsto S &\longmapsto (P \mapsto e_3(S,P)) \times (P \mapsto e_3(S,P)) = (1,\zeta_3). \end{aligned}$$

So if ξ maps $\rho \mapsto r_S S$, then $\{w_3 \circ \iota \circ \xi\}$ maps $\rho \mapsto (1,\zeta_3^{r_S})$. The Kummer isomorphism gives us

$$\begin{aligned} \kappa : H^1(K,\mu_3(\overline{L}_1) \times \mu_3(\overline{L}_2)) &\xrightarrow{\cong} L_1^\times/(L_1^\times)^3 \times L_2^\times/(L_2^\times)^3 \\ \left(\rho \mapsto \left(\frac{\rho(a')}{a'}, \frac{\rho(b')}{b'}\right)\right) &\longleftrightarrow ((a')^3,(b')^3). \end{aligned}$$

Thus

$$\left(\rho \mapsto \left(\frac{\rho(1)}{1}, \frac{\rho(\sqrt[3]{\beta})}{\sqrt[3]{\beta}}\right)\right) \longleftrightarrow (1,\beta)$$

and we see that f is indeed the correct function to take.

Now we prove that g makes the square it is in commute. Let $\{\xi\} \in H^1(K,E[3])$ and recall that we have

$$\begin{aligned} E[3] &\xrightarrow{\phi} \hat{E}[\hat{\phi}] \xrightarrow{\hat{\varepsilon}} \mathbb{Z}/3\mathbb{Z} \\ T, \pm S + T &\mapsto \hat{S} \mapsto 1 (\mathrm{mod}\ 3). \end{aligned}$$

For $R \in E[3]$, let $R = r_S S + r_T T$. Thus if ξ maps $\rho \mapsto R$, then $\varepsilon \circ \phi \circ \xi \in H^1(K,\mathbb{Z}/3\mathbb{Z})$ maps $\rho \mapsto r_T (\mathrm{mod}\ 3)$. The Kummer isomorphism gives us

$$(\rho \mapsto r_T) \longleftrightarrow \alpha \in \left(L_1^\times/(L_1^\times)^3\right)^-$$

where r_T is given by $\zeta_3^{r_T} = \frac{\rho(\sqrt[3]{\alpha})}{\sqrt[3]{\alpha}}$. Going the other way, $\kappa(w_3 \circ \xi)$ is such that if ξ maps $\rho \mapsto R$ then $\kappa(w_3 \circ \xi)$ maps $\rho \mapsto (\zeta_3^{r_T}, *)$, and by the Kummer isomorphism we obtain $(\alpha, *)$, for the same α as

above. We then apply g to 'forget' the second term given by $*$, and g is indeed the correct map to take.

Finally we come to the last square. Let ξ be a 1-cocycle in $H^1(K,\hat{E}[\hat{\phi}])$ corresponding to $\alpha \in (L_1^\times/(L_1^\times)^3)^-$ under the Kummer isomorphism. Let $\xi : \rho \mapsto \xi_\rho \hat{S}$. Then we have $\phi(\xi_\rho T) = \xi_\rho \hat{S}$ and we define $a_{\rho,\mu} = \xi_\rho T + \rho(\xi_\mu T) - \xi_{\rho\mu} T \in \langle S \rangle = E[\phi]$ for all $\rho, \mu \in G$. We can also see $a_{\rho,\mu}$ as an element of μ_3 under the isomorphism $S \mapsto \zeta_3$. Then by [Rot10, Theorem 9.140], $\Delta_2(\xi)$ is given by the crossed product algebra (M,G,a). This algebra is defined as the vector space over M with basis all symbols $\{u_\rho \mid \rho \in G\}$ such that $u_{\mathrm{id}} = \alpha$ and multiplications given by $\beta u_\rho = u_\rho \rho(\beta)$ and $u_\rho u_\mu = a_{\rho,\mu} u_{\rho\mu}$. To show that this is in fact the cyclic algebra $\delta_2(\alpha) = (\chi, \alpha)$, we need to show that $u_\sigma^3 \equiv \alpha \pmod{(L_1^\times)^3}$. We have $u_\sigma^3 = a_{\sigma,\sigma} a_{\sigma^2,\sigma} u_{\mathrm{id}}$ by the law of multiplication. Then we see that

$$a_{\sigma,\sigma} a_{\sigma^2,\sigma} = 3\xi_\sigma S + 3\xi_\sigma T = \mathscr{O} \mapsto 1$$

from which the result follows and the square commutes. □

The following lemma makes the lift from $H^1(K,\hat{E}[\hat{\phi}])$ to $H^1(K,E[3])$ explicit.

Lemma 2.5.9. *Let E be an elliptic curve of the μ_3-nonsplit variety. Let $a \in \left((L_1)^\times/(L_1^\times)^3\right)^-$ where $L_1 = \mathbb{Q}(\zeta_3)$, and $a \in \ker(\delta_2)$. We also have $M = \mathbb{Q}(E[3]) = \mathbb{Q}(\zeta_3, \sqrt[3]{\beta})$ and $L_2 = \mathbb{Q}(\sqrt[3]{\beta})$, for some $\beta \in \mathbb{Q}$. Let $\xi \in M$ be such that $N_{M/L_1}(\xi) = a$. Then a global lift of a to $H^1(K,E[3])$ can be given by (a,b) where*

$$b = \frac{\sigma^2\tau(\xi)\sigma(\xi)}{\sigma^2(\xi)\sigma\tau(\xi)}.$$

Proof. We easily see that this b satisfies all requirements of Lemma 2.5.7. □

2.5.2 $\mathbb{Z}/p\mathbb{Z}$-nonsplit

We are mostly interested in the $p = 3$ case, but we handle this case in a more general way because the case $p = 5$ will turn up in Chapter 8. Let p be an odd prime, then E has a point of order p over K. In this case, the action of G_K on $E[p]$ factors through the subgroup G of $GL_2(\mathbb{Z}/p\mathbb{Z})$ where G consists of all matrices of the form

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}.$$

The following gives a basis for G

$$\sigma \leftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad\qquad \tau \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & g \end{pmatrix}$$

where g is a primitive root of $(\mathbb{Z}/p\mathbb{Z})^\times$, therefore $\tau^{p-1} = \sigma^p = \mathrm{id}$. Thus we can give a basis S,T of $E[p]$ such that

$$\begin{aligned} \sigma(S) &= S & \tau(S) &= S \\ \sigma(T) &= S+T & \tau(T) &= gT \end{aligned}$$

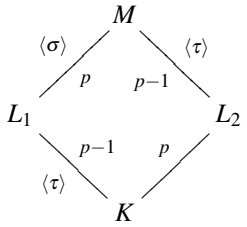
and

$$e_p(S,T) = \zeta_p$$

where e_p is the Weil pairing. We observe that

$$\sigma\tau(T) = gS + gT$$
$$\tau\sigma^g(T) = gS + gT$$

thus $\sigma\tau = \tau\sigma^g$. Let $L_1 = K(\zeta_p)$ and $M = K(T)$, a degree $p(p-1)$ extension of K. Let L_2 be the subfield of M fixed by τ.



(2.18)

We have that $E[\phi] = \langle S \rangle$ and $\hat{E}[\hat{\phi}] = \langle \hat{S} \rangle$ where $\phi(T) = \hat{S}$. We have isomorphisms $\varepsilon : E[\phi] \to \mathbb{Z}/p\mathbb{Z}$ given by $S \mapsto 1 \pmod{p}$ and $\hat{\varepsilon} : \hat{E}[\hat{\phi}] \to \mu_p$ given by $\hat{S} \mapsto \zeta_p$.

Lemma 2.5.10. *The group $H^1(K, E[p])$ is isomorphic to the subgroup H of pairs (a,b) in $K^\times/(K^\times)^p \times M^\times/(M^\times)^p$ such that*

$$\frac{b^g}{\tau(b)} \in (M^\times)^p$$
$$N_{M/L_1}(b) = b\sigma(b)\sigma^2(b)\cdots\sigma^{p-1}(b) \in (L_1^\times)^p$$

and

$$a^i N_{M/L_2}(\sigma^i(b)) = a^i\sigma^i(b)\tau\sigma^i(b)\tau^2\sigma^i(b)\cdots\tau^{p-2}\sigma^i(b) \in (M^\times)^p$$

for each $i \in \{1, \cdots p-1\}$.

Proof. Once again, we must satisfy the conditions of Corollary 2.3.6.

There are p orbits for the action of G_K on $E[p] \setminus \{\mathscr{O}\}$, with representatives iS for $i \in \{1 \ldots p-1\}$, and T. From Section 2.3, we therefore have $H^1(K, E[p]) \subset A^\times/(A^\times)^p$ where

$$A \cong \underbrace{K \times \cdots \times K}_{p-1} \times M.$$

Any element in $H^1(K, E[p])$ represented by $(a_1, a_2, \ldots, a_{p-1}, b)$ will have $a_i \equiv a_1^i \bmod (K^\times)^p$, thus we can represent the element as $(a,b) \in K^\times/(K^\times)^p \times M^\times/(M^\times)^p$.

The first condition of Corollary 2.3.6 is that the element (a,b) must lie in $\ker(g - \sigma_g)$, where g is some primitive root mod p and σ_g is the associated automorphism of A. We have

$$(g - \sigma_g)(a,b) = \left(\frac{a^g}{a^g}, \frac{b^g}{\tau(b)}\right)$$

thus giving the first condition of the lemma.

The second condition of Corollary 2.3.6 involves finding the kernel of some map $\overline{u}$, made explicit in the following way. The set $E[p]^\vee \setminus \{\mathscr{O}\}$ consists of the affine lines in $E[p]$ missing the origin. To define the associated étale algebra, we need to know what these lines look like. From [SS03], we know that we have p^2-1 lines missing the origin. Each such line is given by the set of p points $\{X\}$ satisfying one of the following equations for $i \in \{1,\dots,p-1\}$, where e_p is the Weil pairing.

$$\begin{aligned} e_p(S,X) &= \zeta_p^i \\ e_p(T,X) &= \zeta_p^i \\ e_p(S+T,X) &= \zeta_p^i \\ e_p(2S+T,X) &= \zeta_p^i \\ &\vdots \\ e_p((p-1)S+T,X) &= \zeta_p^i \end{aligned}$$

We now find the Galois orbits of these lines. They are given by the following. First there is one orbit of size $p-1$ containing all the lines with

$$e_p(S,X) = \zeta_p^i. \tag{2.19}$$

Then we have $p-1$ orbits of size p, each represented by a line given by $\{X\}$ such that

$$e_p(T,X) = \zeta_p^i. \tag{2.20}$$

for some i. Thus the étale algebra B associated to $E[p]^\vee \setminus \{\mathscr{O}\}$ is given by

$$B \cong L_1 \times \underbrace{L_2 \times \cdots \times L_2}_{p-1}.$$

Let D be the étale algebra corresponding to the set of all pairs $(P,l) \in (E[p]\setminus\{\mathscr{O}\}) \times (E[p]^\vee \setminus \{\mathscr{O}\})$. Then the map $\overline{u}$ is given by the inclusion of (a,b) into D, followed by the norm from D into B, given by one representative from each of the orbits in (2.19) and (2.20). Thus the first orbit, given by all lines $\{X\}$ such that $e_p(S,X) = \zeta_p^i$ contains the following representative, giving the following condition.

$$(T, S+T, 2S+T, \dots, (p-1)S+T) \longleftrightarrow b\sigma(b)\sigma^2(b)\dots\sigma^{p-1}(b) = N_{M/L_1}(b) \in (L_1^\times)^p$$

Similarly, the other orbits each contain a representative given by the line $\{X\}$ such that $e_p(T,X) = \zeta_p^i$ for some i, leading to the following condition.

$$(iS, iS+T, iS+2T, \dots, iS+(p-1)T) \longleftrightarrow a^i\sigma^i(b)\tau\sigma^i(b)\dots\tau^{p-2}\sigma^i(b) = a^i N_{M/L_2}(\sigma^i(b)) \in (L_2^\times)^p$$

From Corollary 2.3.6, we know that $H^1(K,E[p])$ consists of the intersection of $\ker(g-\sigma_g)$ with $\ker(\overline{u})$, thus we have proved that $H^1(K,E[p]) \cong H$, as required. □

The situation we are in is illustrated by the following diagram. For the last term of the first row, we note that because L_1 contains μ_p, that we can choose an isomorphism $\mu_p \cong \mathbb{Z}/p\mathbb{Z}$ by sending $\zeta_p \mapsto 1$ to obtain $H^2(L_1, \mathbb{Z}/p\mathbb{Z}) \cong H^2(L_1,\mu_p)$. This isomorphism depends on the choice of ζ_p and the details and proof can be found in [GS06, Proposition 4.7.1]. Restricting L_1 to K yields the following Brauer group.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(K,E[\phi]) & \xrightarrow{\iota_*} & H^1(K,E[p]) & \xrightarrow{\phi_*} & H^1(K,\hat{E}[\hat{\phi}]) & \longrightarrow & H^2(K,E[\phi]) \\ \downarrow & & \downarrow & & \downarrow \cong & & \downarrow \cong & & \downarrow \mathrm{Res}_{L_1/K} \\ 0 & \xrightarrow{\delta_1} & L_1^\times/(L_1^\times)^p & \xrightarrow{f} & H & \xrightarrow{g} & K^\times/(K^\times)^p & \xrightarrow{\delta_2} & \mathrm{Br}(L_1) \end{array} \tag{2.21}$$

The maps δ_1, δ_2, f and g are defined as before for sequence (2.17). Of course, this is only useful to us if we have the following theorem.

Theorem 2.5.11. *The diagram 2.21 is commutative.*

The proof of this theorem is very similar to proving that (2.17) is commutative. Once again, by the description of δ_2 and Corollary 2.5.5, the lifting of $a \in H^1(K,\mu_p)$ to $H^1(K,E[3])$ amounts to solving a norm equation. The following lemma makes explicit the lift from $H^1(K,\hat{E}[\hat{\phi}])$ to $H^1(K,E[p])$.

Lemma 2.5.12. *Let E be an elliptic curve of the $\mathbb{Z}/p\mathbb{Z}$-nonsplit variety. Let $a \in K^\times/(K^\times)^p$ such that $a \in \ker(\delta_2)$. We have $L_1 = \mathbb{Q}(\zeta_p)$, $M = \mathbb{Q}(E[p]) = \mathbb{Q}(\zeta_p, \sqrt[p]{\beta})$ and $L_2 = \mathbb{Q}(\sqrt[p]{\beta})$ for some $\beta \in \mathbb{Q}$. Let ξ be such that $N_{M/L_1}(\xi) = a$, and let $\eta = N_{M/L_2}(\xi)$. Then a global lift to $H^1(K,E[3])$ can be given by (a,b) where*

$$b = \frac{\sigma(\eta)\cdot\sigma^2(\eta)^2\cdot\dots\cdot\sigma^{\frac{p-1}{2}}(\eta)^{\frac{p-1}{2}}}{\sigma^{p-1}(\eta)\cdot\sigma^{p-2}(\eta)^2\cdot\dots\cdot\sigma^{\frac{p+1}{2}}(\eta)^{\frac{p-1}{2}}}.$$

Proof. We must satisfy the conditions of Lemma 2.5.10. For the first condition we get, up to pth powers

$$\frac{b^g}{\tau(b)} = \frac{\prod_{i=1}^{p-1}\sigma^i(\eta)^{ig}}{\prod_{j=1}^{p-1}\sigma^{jg^{-1}}(\eta)^j}.$$

Whenever we have $i = jg^{-1}$, then we must also have $j = ig$, and thus the terms in the denominator and numerator cancel out, and the first condition of Lemma 2.5.10 is satisfied. The other conditions can also be shown to be satisfied as follows.

$$\begin{aligned}
b\sigma(b)\sigma^2(b)\dots\sigma^{p-1}(b) &= 1 \\
a^i\sigma^i(b)\tau\sigma^i(b)\tau^2\sigma^i(b)\dots\tau^{p-2}\sigma^i(b) &= \frac{(a^i)^p}{(\xi\,\tau(\xi)\tau^2(\xi)\dots\tau^{p-2}(\xi))^{ip}} && \text{for } i \le \frac{p-1}{2} \\
a^i\sigma^i(b)\tau\sigma^i(b)\tau^2\sigma^i(b)\dots\tau^{p-2}\sigma^i(b) &= \frac{(\xi\,\tau(\xi)\tau^2(\xi)\dots\tau^{p-2}(\xi))^{p(p-i)}}{(a^{p-i-1})^p} && \text{for } i \ge \frac{p+1}{2}
\end{aligned}$$

□

Therefore in the $p = 3$ case, we choose $b = \frac{\sigma(\xi)\sigma\tau(\xi)}{\sigma^2(\xi)\tau\sigma(\xi)}$.

2.5.3 Generic 3-Isogeny

Let E be an elliptic curve of type `Generic3Isogeny`. By Section 2.4, we can write E in the form

$$E : y^2 = x^3 + \Delta(\varepsilon x + \eta)^2$$

with $\varepsilon, \eta, \Delta \in \mathbb{Z}$. The action of G_K on $E[3]$ factors through the subgroup G of $GL_2(\mathbb{Z}/3\mathbb{Z})$ where G consists of all matrices of the form

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

We pick the following generators for G

$$\sigma \leftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \tau \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \qquad \delta \leftrightarrow \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

We choose generators $S,T \in E[3]$ such that

$$\begin{array}{lll} \sigma(S) = S & \tau(S) = S & \delta(S) = 2S \\ \sigma(T) = S+T & \tau(T) = 2T & \delta(T) = 2T \end{array}$$

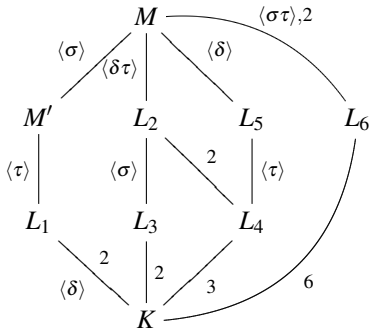
We observe that $\sigma^3 = \tau^2 = \delta^2 = \mathrm{id}$ and

$$\tau\sigma = \sigma^2\tau \qquad \sigma\delta = \delta\sigma \qquad \tau\delta = \delta\tau.$$

Define the fields

$$\begin{aligned} M &= K(E[3]) = K(\zeta_3, \sqrt{\Delta}, \beta) \\ L_1 &= K(S) = K(\sqrt{\Delta}) \\ L_2 &= K(T) = K(\sqrt{-3\Delta}, \beta) \\ L_3 &= K(\sqrt{-3\Delta}) \\ L_4 &= K(\beta) \\ L_5 &= K(\zeta_3, \beta) \end{aligned}$$

with $[M:K] = 12$, $[L_1:K] = 2$ and $[L_2:K] = 6$. Let L_6 be the subfield of M fixed by $\langle \sigma\tau \rangle$. Here, $\beta^3 \in K(\zeta_3)$, however we can show that in fact we can find $\beta^3 \in K$. Because $\delta\tau = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is represented by a diagonal matrix and has two distinct eigenvalues, the basis of the space it operates on can be given by eigenvectors. Thus we have one generator, S, whose coordinates lie in the negative eigenspace of $K(\zeta_3)$, and one generator, T, whose coordinates lie in the positive eigenspace of $K(\zeta_3)$. Thus we have the following diagram.



(2.22)

Let $\phi : E \to \hat{E}$ be the 3-isogeny with kernel generated by S. The analogue of Lemma 2.5.7 can now be given.

Lemma 2.5.13. *The group $H^1(K,E[3])$ is isomorphic to the subgroup H of pairs (a,b) in $L_1^\times/(L_1^\times)^3 \times L_2^\times/(L_2^\times)^3$ satisfying*

$$N_{L_1/K}(a) \in (K^\times)^3,\ N_{L_2/L_3}(b) \in L_3^\times/(L_3^\times)^3 \text{ and } ab\delta\sigma(b) \in L_6^\times/(L_6^\times)^3$$

Proof. We must satisfy the two conditions of Corollary 2.3.6.

There are 2 orbits for the action of G_K on $E[3]\setminus\{\mathcal{O}\}$, with representatives S,T. From Section 2.3, we see that $H^1(K,E[3]) \subset A^\times/(A^\times)^3$ where $A \cong L_1 \times L_2$.

By Corollary 2.3.6, the element (a,b) must lie in $\ker(2-\sigma_2)$ for σ_2 the automorphism sending $S \mapsto -S$ and $T \mapsto -T$. Thus

$$(2-\sigma_2)(a,b) = \left(\frac{a^2}{\delta(a)}, \frac{b^2}{\tau(b)}\right).$$

We must therefore have $a\delta(a) = N_{L_1/K}(a) \in (K^\times)^3$, as well as $b\tau(b) = b\delta(b) = N_{L_2/L_4}(b) \in (L_4^\times)^3$. This final condition depends on the other conditions of the lemma, for

$$\frac{N_{M/L_5}(ab\delta\sigma(b))^2\sigma\left(N_{M/L_5}(ab\delta\sigma(b))\right)}{\sigma^2\left(N_{M/L_5}(ab\delta\sigma(b))\right)} = b\delta(b) \bmod (L_4^\times)^3.$$

The second part of Corollary 2.3.6 involves finding the kernel of some map $\overline{u}$, which we make explicit as follows. The set $E[3]^\vee \setminus \{\mathscr{O}\}$ of affine lines in $E[3]$ missing the origin form two orbits under G_K, represented by

$$(T, S+T, -S+T), (S, T, -S-T). \tag{2.23}$$

The first orbit contains two lines, the second contains six lines, thus the étale algebra corresponding to $E[3]^\vee \setminus \{\mathscr{O}\}$ is $B \cong L_3 \times L_6$. Let D be the étale algebra corresponding to the set of all pairs $(P,l) \in (E[3] \setminus \{\mathscr{O}\}) \times (E[3]^\vee \setminus \{\mathscr{O}\})$. Then $\overline{U}(a,b)$ is given by the inclusion of (a,b) into D, followed by the norm from D into B, given by the two representatives (2.23). Thus we have

$$\begin{aligned}(T, S+T, -S+T) &\longleftrightarrow b\sigma(b)\sigma^2(b) = N_{L_2/L_3}(b) \in (L_3^\times)^3\\ (S, T, -S-T) &\longleftrightarrow ab\delta\sigma(b) \in (L_6^\times)^3.\end{aligned}$$

From Corollary 2.3.6, we see that $H^1(K,E[3])$ consists of the intersection of $\ker(2-\sigma_2)$ with $\ker(\overline{u})$, thus $H^1(K,E[3]) \cong H$, as required. □

The analogue to diagram (2.17) can now be given as

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^1(K,E[\phi]) & \xrightarrow{\iota_*} & H^1(K,E[3]) & \xrightarrow{\phi_*} & H^1(K,\hat{E}[\hat{\phi}]) & \longrightarrow & H^2(K,E[\phi]) \\
\downarrow & & \downarrow & & \downarrow \cong & & \downarrow \cong & & \downarrow \mathrm{Res}_{L_3/K} \\
0 & \xrightarrow{\delta_1} & L_3^\times/(L_3^\times)^3 & \xrightarrow{f} & H & \xrightarrow{g} & (L_1^\times/(L_1^\times)^3)^- & \xrightarrow{\delta_2} & \mathrm{Br}(L_3)
\end{array} \tag{2.24}$$

Once again we need the following theorem.

Theorem 2.5.14. *The diagram* (2.24) *is commutative.*

The proof of this theorem is very similar to proving that (2.17) is commutative, therefore we omit it here. Once again, by the description of δ_2 and Corollary 2.5.5, the lifting of $a \in H^1(K,\hat{E}[\hat{\phi}])$ to $H^1(K,E[3])$ amounts to solving a norm equation over M/M'. The following lemma makes this lift explicit.

Lemma 2.5.15. *Let $E : y^2 = x^3 + \Delta(\varepsilon x + \eta)^2$ be an elliptic curve with a generic 3-isogeny. Let M, M', $L_1, \ldots, L_6$ be defined as in Diagram* (2.22)*. Let σ, δ and τ be as in Section 2.5.3. Let $a \in (L_1^\times/(L_1^\times)^3)^-$ such that $a \in \ker(\delta_2)$. Let $\xi \in M$ be such that $N_{M/M'}(\xi) = a$. Then a global lift of a to $H^1(K,E[3])$ can be given by (a,b) where*

$$b = \frac{\tau\sigma(\xi)\delta\sigma(\xi)\sigma(\xi)\delta\tau\sigma(\xi)}{\xi\,\delta\tau(\xi)\sigma\tau(\xi)\delta\sigma^2(\xi)}$$

Proof. Remembering that $\tau(a) = a$, we easily check all the conditions of Lemma 2.5.13. □

2.6 Practical ways of Computing Certain Selmer groups

Let $\phi : E \to \hat{E}$ be a p-isogeny and $\hat{\phi} : \hat{E} \to E$ its dual. The computational algebra software package MAGMA [BCP97] has an inbuilt function `ThreeIsogenySelmerGroups` which can of course be used to calculate the Selmer groups attached to ϕ and $\hat{\phi}$ in the case when $\phi \circ \hat{\phi} = [3]$. However, in some cases, we can speed up the calculation or we want to consider some p-isogeny where $p \neq 3$. We consider two such cases here.

2.6.1 Case of a Rational p-Torsion Point

Let $E[\phi] \cong \mathbb{Z}/p\mathbb{Z}$ and $\hat{E}[\hat{\phi}] \cong \mu_p$. Then $S^{(\phi)}(E/K)$ consists of all elements $x \in H^1(K, E[\phi])$ such that $x_v \in \mathrm{Im}(\delta_{\phi,v})$, where $\delta_{\phi,v}$ is the local version of the map δ_ϕ from exact sequence (2.3).

We consider the elliptic curves $E = E_\lambda$ with

$$\begin{aligned} &p = 3, \quad E_\lambda : y^2 + xy + \lambda y = x^3 \\ &p = 5, \quad E_\lambda : y^2 + (1-\lambda)xy - \lambda y = x^3 - \lambda x^2. \end{aligned} \tag{2.25}$$

As we see from [Fis03] and Proposition 8.0.1, these are the universal families of elliptic curves over $\overline{K}$ with $(0,0)$ a point of order p. The isogenous curves $\hat{E}_\lambda$ are given by [Vél71] to be

$$\begin{aligned} &p = 3, \quad \hat{E}_\lambda : y^2 + xy + \lambda y = x^3 - 5\lambda x - \lambda(7\lambda + 1) \\ &p = 5, \quad \hat{E}_\lambda : y^2 + (1-\lambda)xy - \lambda y = x^3 - \lambda x^2 - 5\lambda(\lambda^2 + 2\lambda - 1)x - \lambda(\lambda^4 + 10\lambda^3 - 5\lambda^2 + 15\lambda - 1). \end{aligned} \tag{2.26}$$

The images of the local connecting maps are given in the following propositions.

Proposition 2.6.1 ([Fis03, Proposition 1.2])**.** *Let $p = 3$. If $ord_v(\lambda) \geq 0$ then*

$$\mathrm{Im}(\delta_v) = \begin{cases} K_v^\times/(K_v^\times)^3 & \text{if } \mathrm{ord}_v(\lambda) > 0, \\ \mathscr{O}_v^\times/(\mathscr{O}_v^\times)^3 & \text{if } \lambda(27\lambda - 1) \not\equiv 0 \pmod{v} \\ 1 & \text{if } 27\lambda - 1 \equiv 0 \pmod{v}. \end{cases}$$

If $ord_v(\lambda) < 0$ and $v \nmid 3$ then

$$\mathrm{Im}(\delta_v) = \begin{cases} \mathscr{O}_v^\times/(\mathscr{O}_v^\times)^3 & \text{if } 3 \mid \mathrm{ord}_v(\lambda) \\ \langle \lambda \rangle & \text{otherwise.} \end{cases}$$

Proposition 2.6.2 ([Fis03, Proposition 1.4])**.** *Let $p = 5$. Then*

$$\mathrm{Im}(\delta_v) = \begin{cases} K_v^\times/(K_v^\times)^5 & \text{if } \mathrm{ord}_v(\lambda) \neq 0 \\ \mathscr{O}_v^\times/(\mathscr{O}_v^\times)^5 & \text{if } \lambda(\lambda^2 - 11\lambda - 1) \not\equiv 0 \pmod{v} \\ 1 & \text{if } \lambda^2 - 11\lambda - 1 \equiv 0 \pmod{v} \text{ and } v \nmid 5. \end{cases}$$

2.6.2 Split Torsion

In this section, we recall some rank bounds which will be used in Chapter 6 when we search for high rank curves. Following [Fis03], we now take only $K = \mathbb{Q}$. Let $p = 3$ or 5 and let $Y(p)$ be the open subset of the modular curve $X(p)$ obtained by deleting the cusps. Consider the elliptic curves parametrised by $Y(p)$. The $\mathbb{Q}$-points of $Y(p)$ correspond to the classes of triples (E, S, T) where $E/\mathbb{Q}$ is an elliptic curve,

$S, T \in E[p]$, $e_p(S,\ T) = \zeta_p$ and $S \in E(\mathbb{Q})$. We make a choice of coordinate t on $X(p)$ by using equations (2.26) to write

$$\begin{aligned} p = 3, &\quad E = \hat{E}_{t^3/27} \\ p = 5, &\quad E = \hat{E}_{t^5}. \end{aligned} \tag{2.27}$$

where $\hat{E}_\lambda$ is given by (2.26). We then have $E[p] \cong \mu_p \times \mathbb{Z}/p\mathbb{Z}$ as a Galois module, and we have the two isogenies

$$\begin{aligned} E &\xrightarrow{\phi} E' \\ E &\xrightarrow{\psi} E'' \end{aligned}$$

where ϕ is the isogeny with kernel generated by $\langle T \rangle$ and ψ is the isogeny with kernel generated by $\langle S \rangle$. From Section 3.1 of [Fis03], we now obtain the following definitions and theorem.

When $p = 3$, for $t \neq 0, 1$ we define

$$\begin{aligned} \mathscr{P} &= \{v \text{ prime} \mid \operatorname{ord}_v(t/3) > 0\} \\ \mathscr{Q} &= \left\{ v \text{ prime} \mid \begin{array}{r} \left(t^2 + t + 1 \equiv 0 \pmod{v} \text{ and } v \equiv 1 \pmod 3\right) \\ \text{or } (v = 3 \text{ and } \operatorname{ord}_3(t+1) \neq 0) \end{array} \right\} \\ \mathscr{R} &= \left\{ v \text{ prime} \mid \begin{array}{r} (t - 1 \equiv 0 \pmod{v} \text{ and } v \equiv 1 \pmod 3) \\ \text{or } (v = 3 \text{ and } t \equiv 1 \text{ or } 4 \pmod 9) \end{array} \right\}. \end{aligned}$$

When $p = 5$, for $t \neq 0$ we define

$$\begin{aligned} \mathscr{P} &= \{v \text{ prime} \mid \operatorname{ord}_v(t) \neq 0\} \\ \mathscr{Q} &= \left\{ v \text{ prime} \mid \frac{\left((t+1)^5 + 1\right)\left((t-1)^5 + t^5\right)}{(t+2)(2t-1)} \equiv 0 \pmod{v} \text{ and } v \equiv 1 \pmod 5 \right\} \\ \mathscr{R} &= \left\{ v \text{ prime} \mid \begin{array}{r} \left(t^2 - t - 1 \equiv 0 \pmod{v} \text{ and } v \equiv 1 \pmod 5\right) \\ \text{or } (p = 5 \text{ and } t \equiv 3 \pmod 5) \end{array} \right\}. \end{aligned}$$

For every prime $v \in \mathscr{Q} \cup \mathscr{R}$, we can choose nontrivial characters

$$\begin{aligned} \chi_v &: (\mathbb{Z}/v\mathbb{Z})^\times \to \mathbb{Z}/p\mathbb{Z} && \text{if } v \neq p, \\ \chi_p &: (\mathbb{Z}/p^2\mathbb{Z})^\times \to \mathbb{Z}/p\mathbb{Z}. \end{aligned}$$

For $v \in \mathscr{Q}$, these characters must be carefully chosen as follows. In the $v = p = 3$ case, we define

$$\chi_3 : (\mathbb{Z}/9\mathbb{Z})^\times \longrightarrow \mathbb{Z}/3\mathbb{Z} \tag{2.28}$$

$$2 \longmapsto \begin{cases} 1 & \text{if } \operatorname{ord}_3(t+1) < 0 \\ 2 & \text{if } \operatorname{ord}_3(t+1) > 0. \end{cases} \tag{2.29}$$

Otherwise, we have $v \equiv 1 \pmod p$. We may choose $\zeta \in (\mathbb{Z}/v\mathbb{Z})^\times$ an element of order p. In the $p = 3$ case, we have some $\mu \in (\mathbb{Z}/3\mathbb{Z})^\times$ such that $t \equiv \zeta^\mu \pmod v$. In the $p = 5$ case, we write $\phi = 1 + \zeta + \zeta^4$ for the golden ratio, with $\overline{\Phi}$ its conjugate. Then we have some $\mu \in (\mathbb{Z}/5\mathbb{Z})^\times$ such that $t \equiv \zeta^\mu \Phi \pmod v$ or $t \equiv \zeta^\mu \overline{\Phi} \pmod v$. The character we choose must then be given by

$$\chi_v : (\mathbb{Z}/v\mathbb{Z})^\times \longrightarrow \mathbb{Z}/p\mathbb{Z} \tag{2.30}$$

$$x \longmapsto x^{\frac{v-1}{p}} \text{ followed by } \zeta^\mu \longmapsto 1.$$

The $v = p = 5$ case does not occur. The characters χ_v for $v \in \mathbb{Q}$ are called compatible, if they are all chosen to be the same scalar multiple of characters (2.30) and (2.28).

Define the following notation.

$$\begin{aligned}
[\mathscr{A}] &= \left\{\theta \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^p \mid \mathrm{ord}_v(\theta) \equiv 0 \pmod p \text{ for all } v \notin \mathscr{A}\right\} \\
<\mathscr{B}> &= \left\{\chi \in \mathrm{Hom}(G_\mathbb{Q}, \mathbb{Z}/p\mathbb{Z}) \mid \chi_v \text{ is unramified for all } v \notin \mathscr{B}\right\} \\
[\mathscr{A},\mathscr{B}] &= (\chi_q(p))_{p\in\mathscr{A}, q\in\mathscr{B}}.
\end{aligned}$$

From [Fis03] we now obtain the following theorem concerning the Selmer groups we are interested in.

Theorem 2.6.3. *For $E, \hat{E}, \phi, \hat{\phi}$ defined as in this section, and $\mathscr{P}, \mathscr{Q}, \mathscr{R}$ as defined above, we obtain the following.*

$$\begin{aligned}
S^{(\phi)}(E/\mathbb{Q}) &= \{x \in [\mathscr{P}] \mid x_v = 0 \text{ for all } v \in \mathscr{Q}\cup\mathscr{R}\} \\
S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) &= \{x \in <\mathscr{Q}\cup\mathscr{R}> \mid x_v = 0 \text{ for all } v \in \mathscr{P}\}
\end{aligned}$$

These methods of calculating Selmer groups will be used in Chapters 6 and 8.

Following [Fis03], we can also use the definitions made so far to give some upper bounds on the rank of E. The following theorem gives three such upper bounds, known as the Selmer ranks. They are obtained by computing the Cassels-Tate pairing on $S^{(\phi)}(E/\mathbb{Q}) \times S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$, $S^{(\psi)}(E/\mathbb{Q}) \times S^{(\hat{\psi})}(\hat{E}/\mathbb{Q})$, and $S^{(3)}(E/\mathbb{Q})$. These will be used in Chapter 6 when we look for high rank elliptic curves in certain families.

Theorem 2.6.4 ([Fis03])**.** *Let $p = 3$ or 5 and let $E \cong E_t$ as in* (2.27)*. Let ϕ be the isogeny with kernel generated by $\langle T\rangle$ and ψ the isogeny with kernel generated by $\langle S\rangle$. Define the matrices*

$$\begin{aligned}
\Xi_\phi &= \begin{pmatrix} [\mathscr{P},\mathscr{Q}] & [\mathscr{P},\mathscr{R}] \end{pmatrix} \\
\Xi_\psi &= \begin{pmatrix} [\mathscr{P},\mathscr{R}] \\ [\mathscr{Q},\mathscr{R}] \end{pmatrix} \\
\Xi_p &= \begin{pmatrix} 0 & [\mathscr{P},\mathscr{Q}] & [\mathscr{P},\mathscr{R}] \\ -[\mathscr{P},\mathscr{Q}]^T & [\mathscr{Q},\mathscr{Q}]-[\mathscr{Q},\mathscr{Q}]^T & [\mathscr{Q},\mathscr{R}] \\ -[\mathscr{P},\mathscr{R}]^T & -[\mathscr{Q},\mathscr{R}]^T & 0 \end{pmatrix}.
\end{aligned}$$

Then we have three rank estimates for $E(\mathbb{Q})$ given by

$$\begin{aligned}
r_\phi &= |\mathscr{P}| + |\mathscr{Q}| + |\mathscr{R}| - 1 - 2\cdot\mathrm{rank}(\Xi_\phi) \\
r_\psi &= |\mathscr{P}| + |\mathscr{Q}| + |\mathscr{R}| - 1 - 2\cdot\mathrm{rank}(\Xi_\psi) \\
r_p &= |\mathscr{P}| + |\mathscr{Q}| + |\mathscr{R}| - 1 - \mathrm{rank}(\Xi_p).
\end{aligned}$$

2.7 Rank Estimates

In this section, we see how we may use the information contained in this chapter to give an upper bound on the rank of an elliptic curve. This will be used in Chapters 6 and 7, where we search for high rank curves. Our references are [Cre12, Fis14, Ser79]. Let $\phi : E \to \hat{E}$ be an isogeny of degree p, and $\hat{\phi} : \hat{E} \to E$ its dual.

By the exact sequence (2.1) we obtain the following formula describing the rank of E. Consider all the groups as being $\mathbb{F}_p$-vector spaces.

$$\text{rank}(E(K)) = \dim \frac{\hat{E}(K)}{\phi(E(K))} + \dim \frac{E(K)}{\hat{\phi}(\hat{E}(K))} - \dim E(K)[\phi] - \dim \hat{E}(K)[\hat{\phi}] \tag{2.31}$$

Therefore our task is now to determine as accurately as possible the values of $\dim \frac{\hat{E}(K)}{\phi(E(K))}$ and $\dim \frac{E(K)}{\hat{\phi}(\hat{E}(K))}$. Using exact sequence (2.6), we could approximate $\dim \frac{\hat{E}(K)}{\phi(E(K))}$ by the number of generators of $S^{(\phi)}(E/K)$, and we could even determine it exactly if we knew which elements of $S^{(\phi)}(E/K)$ are mapped to nontrivial elements of $Ш(E/K)[\phi]$. From exact sequence (2.6) and formula (2.31) we therefore obtain the following formula for the rank r_E of E.

$$p^{r_E} = \frac{|S^{(\phi)}(E/K)| \cdot |S^{(\hat{\phi})}(\hat{E}/K)|}{|E(K)[\phi]| \cdot |\hat{E}(K)[\hat{\phi}]| \cdot |Ш(E/K)[\phi]| \cdot |Ш(\hat{E}/K)[\hat{\phi}]|} \tag{2.32}$$

We are left with determining which elements of $S^{(\phi)}(E/K)$ are mapped to nontrivial elements of $Ш(E/K)[\phi]$. We will need the following tool to help us do so. In [Cas62], Cassels constructed an alternating bilinear pairing

$$< , >: Ш(E/K) \times Ш(E/K) \to \mathbb{Q}/\mathbb{Z} \tag{2.33}$$

which can be used to improve the upper bound on the rank of an elliptic curve. It is called the Cassels-Tate pairing and will be explored in great detail in Chapter 3. It has several important properties.

Theorem 2.7.1. *Let $\phi, \hat{\phi}$ and $E, \hat{E}$ be as above. Then the following two properties hold.*

1. $< \phi(x), y > = < x, \hat{\phi}(y) >$ *for all* $x \in Ш(E/K)$ *and* $y \in Ш(\hat{E}/K)$.
2. $y \in Ш(E/K)$ *is in the image of* $\hat{\phi} : Ш(\hat{E}/K) \to Ш(E/K)$ *if and only if* $< x, y >= 0$ *for all* x *in the kernel of* $\phi : Ш(E/K) \to Ш(\hat{E}/K)$.

Because of exact sequence (2.6), we see that it makes sense to evaluate the pairing on elements of Selmer groups. We shall be using this pairing to compute upper bounds on ranks of elliptic curves throughout this thesis. Usually we will be in the following situation. Let $\hat{M}$ denote the matrix representing the Cassels-Tate pairing on $S^{\hat{\phi}}(\hat{E}/K)$. Then we have

$$p^{r_E} \leq \frac{|S^{(\phi)}(E/K)| \cdot |S^{(\hat{\phi})}(\hat{E}/K)|}{|E(K)[\phi]| \cdot |\hat{E}(K)[\hat{\phi}]| \cdot p^{\text{Rank}(\hat{M})}}. \tag{2.34}$$

We can go even further. We now construct a sequence of 'Selmer groups', all of which contain either $\hat{E}(K)/\phi(E(K))$ or $E(K)/\hat{\phi}(\hat{E}(K))$, to help us make use of (2.31). Let $S_1 = S^{(\phi)}(E/K)$ and $\hat{S}_1 = S^{(\hat{\phi})}(\hat{E}/K)$. Define S_i as follows

- if i is even, $i = 2n$, and $S_i = \text{Im}\left(S^{(p^n)}(\hat{E}/K) \to S_1\right)$
- if i is odd, $i = 2n+1$ and $S_i = \text{Im}\left(S^{(p^n\phi)}(E/K) \to S_1\right)$.

The subspaces $\hat{S}_i$ are defined in the same way, swapping over the roles of E and $\hat{E}$. Then we have the following inclusions

$$\frac{\hat{E}(K)}{\phi(E(K))} \subset \cdots \subset S_3 \subset S_2 \subset S_1 = S^{(\phi)}(E/K) \tag{2.35}$$

$$\frac{E(K)}{\hat{\phi}(\hat{E}(K))} \subset \cdots \subset \hat{S}_3 \subset \hat{S}_2 \subset \hat{S}_1 = S^{(\hat{\phi})}(\hat{E}/K). \tag{2.36}$$

The Cassels-Tate pairing (3.6) now induces the following pairings, as taken from [Fis14].

Theorem 2.7.2 ([Fis14, Theorem 2.1])**.** *Let $m \geq 1$ be an integer.*

1. *If m is odd then there are alternating pairings*

$$\theta_m : S_m \times S_m \to \mathbb{F}_p \text{ and } \hat{\theta}_m : \hat{S}_m \times \hat{S}_m \to \mathbb{F}_p$$

   with kernels S_{m+1} and $\hat{S}_{m+1}$.

2. *If m is even then there is a pairing*

$$\theta_m : S_m \times \hat{S}_m \to \mathbb{F}_p$$

   with left kernel S_{m+1} and right kernel $\hat{S}_{m+1}$.

Thus by doing a descent by p-isogeny and calculating Cassels-Tate pairings, we obtain ever more accurate bounds on the dimensions of $\hat{E}(K)/\phi(E(K))$ and $E(K)/\hat{\phi}(\hat{E}(K))$. The rest of this thesis will be devoted to calculating the Cassels-Tate pairing in a variety of settings. The next chapter is devoted entirely to defining the pairing and proving its most important properties. The theorems in this section were used in Chapter 6 to give rank upper bounds for large numbers of elliptic curves.

Chapter 3

The Cassels-Tate Pairing

In this chapter, we discuss the main object of study of this thesis, namely the Cassels-Tate pairing. We shall first discuss the Weil pairing definition, as used by Cassels in his original papers [Cas59, Cas62], and then move on to an alternative definition, which we will be using for most of this thesis. There are computational reasons for preferring one definition over another.

3.1 The Weil Pairing Definition

Let K be a number field, and p a prime. Let E/K be an elliptic curve admitting a p-isogeny. Thus we have

$$E \xrightarrow{\phi} \hat{E} \xrightarrow{\hat{\phi}} E$$

where $\hat{\phi} \circ \phi = [p]$, the multiplication-by-$p$ map. In this section we construct the Cassels-Tate pairing on part of the Tate-Shafarevich group $Ш(\hat{E}/K)$, and prove some fundamental results about it.

Theorem 3.1.1. *There is an alternating bilinear pairing*

$$Ш(\hat{E}/K) \times Ш(\hat{E}/K) \to \mathbb{Q}/\mathbb{Z}$$

whose kernel is the subgroup of infinitely divisible elements.

There are various ways of defining this pairing. The first definition we consider defines the pairing on part of $Ш(\hat{E}/K)$ and is one of the definitions considered by Poonen and Stoll in [PS98]. As an abstract group, $E[\phi] \cong \mathbb{Z}/p\mathbb{Z}$, therefore we can choose some $T \in E[\phi]$ that generates the whole group. In order to define the Weil pairing we will need the following result.

Proposition 3.1.2 ([Sil08, III.3.5])**.** *Let E be and elliptic curve and let $A = \sum n_P(P) \in \mathrm{Div}(E)$. Then A is a principal divisor if and only if*

$$\sum_{P \in E} n_P = 0 \text{ and } \sum_{P \in E} [n_P]P = \mathscr{O}.$$

Applying Proposition 3.1.2 to our case, there exists a function $f \in \overline{K}(E)$ such that

$$\mathrm{div}(f) = p \cdot (T) - p \cdot (\mathscr{O}).$$

Now we take $\hat{T} \in \hat{E}$ such that $\hat{\phi}(\hat{T}) = T$. Then there also exists a function $g \in \overline{K}(\hat{E})$ such that

$$\begin{aligned} \operatorname{div}(g) &= \phi^*(T) - \phi^*(\mathscr{O}) \\ &= \sum_{R \in \hat{E}[\hat{\phi}]} (\hat{T} + R) - (R). \end{aligned} \tag{3.1}$$

We easily verify that the functions $f \circ \hat{\phi}$ and g^p have the same divisor, namely

$$\operatorname{div}(f \circ \hat{\phi}) = \operatorname{div}(g^p) = p \cdot \left(\sum_{R \in \hat{E}[\hat{\phi}]} (\hat{T} + R) \right) - p \cdot \left(\sum_{R \in \hat{E}[\hat{\phi}]} (R) \right).$$

Therefore by multiplying by a suitable constant in $\overline{K}^\times$, we can assume that

$$f \circ \hat{\phi} = g^p.$$

Now we take $S \in \hat{E}[\hat{\phi}]$ to be a $\hat{\phi}$-torsion point. Then for any point $X \in \hat{E}$, we have

$$g(X+S)^p = f(\hat{\phi}(X) + \hat{\phi}(S)) = f(\hat{\phi}(X)) = g(X)^p.$$

Thus, considered as a function of X, the function $\frac{g(X+S)}{g(X)}$ takes its values in μ_p. It is also a constant function because the morphism

$$\hat{E} \to \mathbb{P}^1, \quad S \mapsto \frac{g(X+S)}{g(X)}$$

is not surjective. Therefore, we can now define the Weil pairing to be the following.

Definition 3.1.3. The Weil pairing is defined as

$$e_\phi : E[\phi] \times \hat{E}[\hat{\phi}] \to \mu_p$$

where $e_\phi(T,S) = \frac{g(X+S)}{g(X)}$ and $X \in E$ is any suitable point.

This pairing is bilinear, alternating, nondegenerate and Galois invariant. These properties can be proved in a similar way as is done in [Sil08, Proposition III.8.1].

To define the global pairing in Theorem 3.1.1 we need a local pairing called the *local Tate pairing*. Let K_v denote the localisation of K at some place v, then the Weil pairing induces a cup product

$$\cup : H^1(K_v, E[\phi]) \times H^1(K_v, \hat{E}[\hat{\phi}]) \to H^2(K_v, E[\phi] \otimes \hat{E}[\hat{\phi}])$$

where $(\xi \cup \eta)(\sigma,\tau) = \xi(\sigma) \otimes \eta(\tau)^\sigma$ by the definition of the cup product. We now want to replace the final group with something more manageable. From the Weil pairing, we know that $E[\phi] \otimes \hat{E}[\hat{\phi}] \cong \mu_p$, therefore for non-archimedean places v we can apply the invariant map $\operatorname{inv}_{K_v} : \operatorname{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$ from local class field theory [CF67]. For v a finite place, the final group can therefore be replaced by the following:

$$H^2(K_v, E[\phi] \otimes \hat{E}[\hat{\phi}]) \cong H^2(K_v, \mu_p) \cong \frac{1}{p}\mathbb{Z}/\mathbb{Z}$$

and thus we obtain a pairing map.

Definition 3.1.4. The *local Tate pairing* is defined as

$$<,>_{v,e_\phi}: H^1(K_v,E[\phi]) \times H^1(K_v,\hat{E}[\hat{\phi}]) \to \mathbb{Q}/\mathbb{Z}$$

given by $< x,y >_{v,e_\phi} = \text{inv}_{K_v}\{e_\phi(\xi(\sigma),\eta(\tau)^\sigma)\}$ where $x = \{\xi(\sigma)\}_\sigma$ and $y = \{\eta(\tau)\}_\tau$.

We can now define the global Cassels-Tate pairing. This pairing is defined on

$$Ш(\hat{E}/K) \times Ш(\hat{E}/K) \to \mathbb{Q}/\mathbb{Z}.$$

Let $x,y \in Ш(\hat{E}/K)$. We shall define the pairing only in the special case that $y \in Ш(\hat{E}/K)[\hat{\phi}]$, thus by the exact sequence

$$0 \to E(K)/\hat{\phi}(\hat{E}(K)) \to S^{(\hat{\phi})}(\hat{E}/K) \to Ш(\hat{E}/K)[\hat{\phi}] \to 0 \tag{3.2}$$

we can lift y to some element η in the Selmer group $S^{(\hat{\phi})}(\hat{E}/K)$. This is one of the elements we will use in the pairing. We need a lemma to proceed with the definition.

Lemma 3.1.5. *For any $x \in Ш(\hat{E}/K)$, we can find some lift $x_1 \in H^1(K,E)$ such that $\phi(x_1) = x$.*

Proof. From the short exact sequence

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} \hat{E} \longrightarrow 0$$

we take Galois cohomology in both the global and local case to obtain the following exact sequences.

$$\begin{array}{ccccccccc} \hat{E}(K) & \xrightarrow{\delta_\phi} & H^1(K,E[\phi]) & \xrightarrow{\iota_\phi} & H^1(K,E) & \xrightarrow{\phi} & H^1(K,\hat{E}) & \longrightarrow & H^2(K,E[\phi]) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \prod_v \hat{E}(K_v) & \xrightarrow{\{\delta_{\phi,v}\}} & \prod_v H^1(K_v,E[\phi]) & \xrightarrow{\{\iota_{\phi,v}\}} & \prod_v H^1(K_v,E) & \xrightarrow{\phi} & \prod_v H^1(K_v,\hat{E}) & \to & \prod_v H^2(K_v,E[\phi]) \end{array} \tag{3.3}$$

We know that x is locally trivial, thus it maps to 0 in $H^2(K_v,E[\phi])$. If we can show that it is also mapped to 0 in $H^2(K,E[\phi])$, then it belongs to the image of ϕ.

By making a finite extension L/K of degree n, prime to p, we can ensure that $E[\phi] \cong \mu_p$ over L, thus we have $H^2(L,E[\phi]) \cong \text{Br}(L)[p]$. Let v be a place of K. Then we have the following commutative diagram.

$$\begin{array}{ccccc} H^2(K,E[\phi]) & \xrightarrow{\text{Res}} & H^2(L,E[\phi]) \cong \text{Br}(L)[p] & \xrightarrow{\text{Cor}} & H^2(K,E[\phi]) \\ \downarrow{\scriptstyle \text{loc}_1} & & \downarrow{\scriptstyle \text{loc}_2} & & \downarrow{\scriptstyle \text{loc}_1} \\ H^2(K_v,E[\phi]) & \xrightarrow{\text{Res}} & \oplus_{w|v} H^2(L_w,E[\phi]) \cong \oplus_{w|v}\text{Br}(L_w)[p] & \xrightarrow{\text{Cor}} & H^2(K_v,E[\phi]) \end{array} \tag{3.4}$$

By global class field theory, the following exact sequence holds for any number field L.

$$0 \longrightarrow \text{Br}(L) \longrightarrow \bigoplus_w \text{Br}(L_w) \xrightarrow{\Sigma \text{inv}_w} \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \tag{3.5}$$

Thus the map loc_2 in (3.4) is injective. We also know that Cor$\circ$Res$=[n]$ [GS06, Proposition 3.3.7]. We will now show that loc_1 is also injective. For any $u \in H^2(K_v,E[\phi])$, there is a unique $\chi \in H^2(L,E[\phi])$ such that $\text{loc}_2(\chi) = \text{Res}(u)$. Thus because $\text{GCD}(p,n) = 1$, $\text{Cor}(\chi)$ is the unique lift of $n \cdot u$ to $H^2(K,E[\phi])$. We have therefore shown that loc_1 is injective, therefore x is in the kernel of $H^1(K,\hat{E}) \to H^2(K,E[\phi])$ and there exists $x_1 \in H^1(K,E)$ such that $\phi(x_1) = x$. □

We also know that because x is in $Ш(\hat{E}/K)$, it is locally trivial, so by the exact complex (3.3) we can find some element $\xi_v \in H^1(K_v, E[\phi])$ such that $-\xi_v$ and x_1 have the same image in $H^1(K_v, E)$. The pairing is now defined as follows.

Definition 3.1.6 (Weil pairing definition of the Cassels-Tate pairing)**.** Let $x \in Ш(\hat{E}/K)$ and $y \in Ш(\hat{E}/K)[\hat{\phi}]$. The Cassels-Tate pairing is defined as

$$< x, y >_{CT} = \sum_{v \in M_K} < \xi_v, \eta_v >_{v, e_\phi} \tag{3.6}$$

where $< , >_{v,e_\phi}$ is the local Tate pairing from Definition 3.1.4. The element ξ_v is as described above, and η_v is the localisation of η, obtained from lifting y to some element η in the Selmer group $S^{(\hat{\phi})}(\hat{E}/K)$.

The following theorems establish this definition as a legitimate and useful one.

Theorem 3.1.7. *The Cassels-Tate pairing is independent of the choices of x_1, ξ_v and η made during its construction.*

Proof. From (3.5), it follows that the local Tate pairing in Definition 3.1.4 satisfies a product formula. Thus if $a \in H^1(K, E[\phi])$ and $b \in H^1(K, \hat{E}[\hat{\phi}])$ then we have

$$\sum_v < a_v, b_v >_{v, e_\phi} = 0. \tag{3.7}$$

If we make a different choice for x_1, say x_1', then x_1' differs from x_1 by an element in the image of

$$H^1(K, E[\phi]) \xrightarrow{\iota_\phi} H^1(K, E).$$

Because η is an element of $H^1(K, \hat{E}[\hat{\phi}])$, it follows from the product formula that the choice of x_1 does not influence the Cassels-Tate pairing.

From an instance of Tate local duality [Ser02, Theorem 2.5.2], we know that im $\delta_{\phi,v}$ and im $\delta_{\hat{\phi},v}$ are exact annihilators with respect to the local Tate pairing. We have $\eta \in H^1(K, \hat{E}[\hat{\phi}])$ such that it is in ker $\iota_{\hat{\phi},v}$ for all places v, thus it lies in im $\delta_{\hat{\phi},v}$. If we change the choice of ξ_v, it must be by an element in the kernel of $\iota_{\phi,v}$, which is the image of $\delta_{\phi,v}$. Thus it does not matter for the local pairing which choice of ξ_v we make.

To show that the choice of η also does not influence the outcome, we need to define another local pairing, which is due to Tate. From Proposition 3.1.2 we get the exact sequence

$$0 \longrightarrow \overline{K}_v(E)^\times / \overline{K}_v^\times \xrightarrow{\text{div}} \text{Div}^0(E) \xrightarrow{\text{sum}} E \longrightarrow 0$$

and take Galois cohomology to obtain

$$H^1(K_v, E) \xrightarrow{\delta} H^2(K_v, \overline{K}_v(E)^\times / \overline{K}^\times) \xrightarrow{\text{div}} H^2(K_v, \text{Div}^0(E))$$

The local pairing is now defined as

$$\begin{aligned} E(K_v) \times H^1(K_v, E) &\longrightarrow \mathbb{Q}/\mathbb{Z} \\ (x, y)_v &\longmapsto -\text{inv} f(\mathfrak{x}) \end{aligned}$$

where $\text{sum}(\mathfrak{x}) = x$ and $f = \delta(y)$. By [Fis03, Proposition 2.1], if $\eta \in H^1(K_v, \hat{E}[\hat{\phi}])$ with $\delta_{\hat{\phi},v} : x \mapsto a$ and $\iota_{\hat{\phi},v} : \eta \mapsto y$ then $< a, \eta >_{v,e_\phi} = (x, y)_v$. By (3.5), the pairing $(,)_v$ also satisfies a product formula. If we

change the choice of η, say to η', then η' differs from η by an element in the image of $\delta_{\hat{\phi}}$. Thus there exists some $P \in E(K)$ such that $\eta' = \eta + \delta_{\hat{\phi}}(P)$. This changes the pairing (3.6) by

$$\sum_v (\xi_v, \delta_{\hat{\phi}}(P))_v = \sum_v (x_1, P)_v.$$

Since x_1 and P are both global elements, the product formula for $(\ ,\ )_v$ gives us that $\sum_v (x_1,P)_v = 0$. Thus the Cassels-Tate pairing is independent of the choice of η. □

It looks at the moment as though the pairing is given by an infinite sum. This is not the case, as we will show later in Proposition 3.3.6, for a variation of the definition. The following theorem is a very well-known result, and we refer to [Fis03, Theorem 2] for a proof.

Theorem 3.1.8. *The Cassels-Tate pairing in Definition 3.1.6 is an alternating bilinear pairing whose kernel is the subgroup of infinitely divisible elements.*

The following theorem is part of the proof of Theorem 3.1.8, and we include it here to highlight this result.

Theorem 3.1.9 ([Fis03, Theorem 3])**.** *Let $\phi : E \to \hat{E}$ be an isogeny of elliptic curves over K. Then $x \in Ш(\hat{E}/K)$ belongs to the image of $\phi : Ш(E/K) \to Ш(\hat{E}/K)$ if and only if $< x, y >_{CT} = 0$ for all $y \in Ш(\hat{E}/K)[\hat{\phi}]$.*

The Cassels-Tate pairing lifts naturally to a pairing

$$S^{(\hat{\phi})}(\hat{E}/K) \times S^{(\hat{\phi})}(\hat{E}/K) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

whose kernel is the image of $S^{(p)}(E/K)$. The description of this kernel follows directly from Theorem 3.1.9. For the explicit calculations we shall be doing later, we need a slight modification of the definition in this case. We must replace (3.3) by the version coming from the short exact sequence

$$0 \longrightarrow E[\phi] \longrightarrow E[p] \xrightarrow{\phi} \hat{E}[\hat{\phi}] \longrightarrow 0$$

of which we take Galois cohomology in both the global and local cases to obtain the following exact sequences.

$$\begin{array}{ccccccccc}
\hat{E}(K)[\hat{\phi}] & \xrightarrow{\delta_\phi} & H^1(K,E[\phi]) & \xrightarrow{\iota_\phi} & H^1(K,E[p]) & \xrightarrow{\phi} & H^1(K,\hat{E}[\hat{\phi}]) & \longrightarrow & H^2(K,E[\phi]) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
\prod_v \hat{E}(K_v)[\hat{\phi}] & \xrightarrow{\{\delta_{\phi,v}\}} & \prod_v H^1(K_v,E[\phi]) & \xrightarrow{\{\iota_{\phi,v}\}} & \prod_v H^1(K_v,E[p]) & \xrightarrow{\phi} & \prod_v H^1(K_v,\hat{E}[\hat{\phi}]) & \to & \prod_v H^2(K_v,E[\phi])
\end{array} \tag{3.8}$$

The analogue of Lemma 3.1.5 is then the following.

Lemma 3.1.10. *For any $x \in S^{(\hat{\phi})}(\hat{E}/K)$, we can find some lift $x_1 \in H^1(K,E[p])$ such that $\phi(x_1) = x$.*

Proof. The proof is very similar to that of Lemma 3.1.5 and is therefore omitted. □

We then find some $\xi_v \in H^1(K_v,E[\phi])$ such that ξ_v and x_1 have the same image in $H^1(K_v,E[p])$, and the rest of the definition of the Cassels-Tate pairing remains the same. Thus the Cassels-Tate pairing can be used to determine which elements of $S^{(\hat{\phi})}(\hat{E}/K)$ can be lifted to elements of $S^{(p)}(E/K)$. This allows us to turn a descent by p-isogeny into a full p-descent, and thus potentially improves rank estimates of elliptic curves. In Chapter 6, we shall use it in just this way to search for high rank curves in families of elliptic curves with prescribed torsion groups.

3.2 Computing the Local Pairing

In Section 3.1, we saw that to compute the Cassels-Tate pairing, we must take the sum over a number of local Tate pairings. In this section, we will show how such local pairings may be explicitly computed.

In this section, let p be some prime, K a global field with $\mu_p \subset K$, and v some place of K. Let us fix some chosen root of unity ζ_p. Recall from local class field theory that for any local field K_v we have the invariant map

$$\mathrm{inv}_{K_v} : \mathrm{Br}(K_v) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

Let E/K be an elliptic curve and $\phi : E \to \hat{E}$ an isogeny of degree p, with $\hat{\phi} : \hat{E} \to E$ its dual such that $\phi \circ \hat{\phi} = [p]$. We seek to compute explicitly the local Tate pairing from Definition 3.1.4. Let $E[\phi] = \langle S \rangle$ and $\hat{E}[\hat{\phi}] = \langle \hat{T} \rangle$ such that the Weil pairing (see Definition 3.1.3) gives $e_\phi(S, \hat{T}) = \zeta_p$. By making some extension L_w/K_v of degree n prime to p, we can ensure that $E[\phi] \cong \mu_p$ and $\hat{E}[\hat{\phi}] \cong \mu_p$, and we choose these isomorphisms such that we keep invariant $e_\phi(S, \hat{T}) = \zeta_p$. We then have $H^1(L_w, E[\phi]) \cong H^1(L_w, \hat{E}[\hat{\phi}]) \cong L_w^\times/(L_w^\times)^p$. This leads us to consider the following diagram. Note that the vertical restriction maps depend on the isomorphisms chosen earlier.

$$\begin{array}{lccccccc}
<\ ,\ >_{v,e_\phi}: & H^1(K_v, E[\phi]) & \cup & H^1(K_v, \hat{E}[\hat{\phi}]) & \longrightarrow & H^2(K_v, \mu_p) & \xrightarrow{\mathrm{inv}_{K_v}} & \frac{1}{p}\mathbb{Z}/\mathbb{Z} \\
 & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & & \downarrow n \\
\{\ ,\ \}_v: & L_w^\times/(L_w^\times)^p & \cup & L_w^\times/(L_w^\times)^p & \longrightarrow & H^2(L_w, \mu_p) & \xrightarrow{\mathrm{inv}_{L_w}} & \frac{1}{p}\mathbb{Z}/\mathbb{Z}
\end{array} \tag{3.9}$$

From [CF67, Proposition IV.7.9(iii)], we know that

$$\mathrm{Res}(a \cup b) = \mathrm{Res}(a) \cup \mathrm{Res}(b)$$

for all $a \in H^1(K_v, E[\phi])$ and $b \in H^1(K_v, \hat{E}[\hat{\phi}])$. From [CF67, Theorem VI.1.3], we find

$$\mathrm{inv}_{L_w} \circ \mathrm{Res} = n \cdot \mathrm{inv}_{K_v}.$$

Remark 3.2.1. Thus whenever we must extend K_v to L_w, this has the effect of multiplying our final solution by n. Because n is prime to p, we can recover the desired solution.

We now proceed to define the Hilbert norm residue symbol, and show how it may be used.

Definition 3.2.2. Let $\mu_p \subset K$, where K is some global field. For $a, b \in K^\times$, and v any prime of K, let G be the Galois group for the Kummer extension $K(\sqrt[p]{a})/K$. The *Hilbert norm residue symbol* is defined as

$$(a,b)_v = \frac{(\sqrt[p]{a})^{\psi_v(b)}}{\sqrt[p]{a}}$$

where $\psi_v : K_v^\times \to G_v$ is the local Artin map associated with the extension $K(\sqrt[p]{a})/K$.

The first thing we need is that this definition coincides with the cup product construction in (3.9).

Proposition 3.2.3. $\zeta_p^{p \cdot \{a,b\}_v} = (a,b)_v$

Proof. This follows from [Ser79, Proposition XIV.2.6]. □

Remark 3.2.4. Let $K = \mathbb{Q}(\mu_p)$ for some prime p, and v a prime that splits over K, not necessarily completely, thus giving us $(v) = \mathscr{P}_1 \cdot \ldots \cdot \mathscr{P}_n$. Then there are n embeddings of ζ_p into $\mathbb{Q}_v(\mu_p)$, each one corresponding to one of the primes $\mathscr{P}_i$. If we choose some primitive root of unity ζ_p, we can define the map

$$\mathrm{Ind}_{\zeta_p}(\zeta_p') = u$$

where $u \in \frac{1}{p}\mathbb{Z}/\mathbb{Z}$ such that $\zeta_p^{pu} = \zeta_p'$. Let $\zeta_p^{(\mathscr{P}_i)}$ correspond to the choice of prime $\mathscr{P}_i$. Then $\mathrm{Ind}_{\zeta_p^{(\mathscr{P}_i)}} \circ (\ ,\ )_{\mathscr{P}_i}$ does not depend on the choice of ζ_p, and therefore the pairings at $\mathscr{P}_i$ and $\mathscr{P}_j$ will be the same for all $i, j \in \{1, \ldots, n\}$. Therefore we need only calculate one such pairing and multiply it by n. Thus in the case $p = 3$, any prime v with $v = 1 \pmod 3$ splits and we multiply the final answer obtained at $\mathscr{P}_1$ by 2.

Thus we are now able to compute all local pairings. We simply extend the field K if necessary, and use the Hilbert norm residue symbol in our calculations. To make this calculation explicit, we need to define one more symbol.

Definition 3.2.5. Let K be a global field with $\mu_m \subset K$ for some natural number m. Let $\mathbf{p}$ be a prime ideal such that m and $\mathbf{p}$ are coprime. Then the *power residue symbol* $\left(\frac{a}{\mathbf{p}}\right)$ is defined as the unique mth root of 1 such that

$$\left(\frac{a}{\mathbf{p}}\right) \equiv a^{\frac{N\mathbf{p}-1}{m}} \pmod{\mathbf{p}}.$$

The following propositions serve to make this calculation completely explicit.

Proposition 3.2.6. *Let K be a global field with $\mu_m \subset K$. Let $a, b \in K^\times$, and v a place of K. Let S denote the set of primes of K consisting of the archimedean ones together with those dividing p. Then the following properties hold.*

1. $(a,b)_v(a,c)_v = (a,bc)_v$
2. $(a,b)_v = 1$ *if either a or $b \in (K_v^\times)^m$.*
3. $(a,b)_v = 1$ *if b is a norm for the extension $K_v(\sqrt[m]{a})/K_v$.*
4. $(a,b)_v = 1$ *if $a+b \in (K_v^\times)^m$, in particular $(a,-a)_v = 1 = (a,1-a)_v$.*
5. $(a,b)_v(b,a)_v = 1$.
6. *If $v \notin S$, then $(a,b)_v = \left(\frac{c}{v}\right)$ where $c = (-1)^{\mathrm{val}_v(a)\mathrm{val}_v(b)} a^{\mathrm{val}_v(b)} b^{-\mathrm{val}_v(a)}$.*

Proof. The proof of these statements is given by [Gra03, Proposition II.7.1.1]. □

The previous proposition can be used to compute $(a,b)_v$ explicitly whenever $v \nmid p$. We now turn to the case that $v \mid p$, for which we follow [CF67, Exercise 2]. Let $K = \mathbb{Q}(\zeta_p)$. Then p is totally ramified in K and $\lambda = 1 - \zeta_p$ generates the prime ideal corresponding to the unique prime v of K lying over p. We define the group of units

$$U_i = \left\{ x \in K_v^\times \mid x \equiv 1 (\mathrm{mod}\ \lambda^i) \right\}, i = 1, 2, \ldots$$

The image of $\eta_i = 1 - \lambda^i$ then generates U_i/U_{i+1}, which is cyclic of order p, and the image of λ generates $K_v^\times/(K_v^\times)^p U_1$. Because we have that $U_{p+1} \subset (K_v^\times)^p$, it follows that the elements

$$\lambda, \zeta_p = \eta_1, 1 - \lambda^2 = \eta_2, \ldots, 1 - \lambda^p = \eta_p$$

generate $K_v^\times/(K_v^\times)^p$. These generators are independent, because the order of this group must be $p^2/|p|_v = p^{1+p}$. The following properties now hold.

Proposition 3.2.7. *For η_i defined before, the following properties hold.*

1. $(\eta_i,\eta_j)_v = (\eta_i,\eta_{i+j})_v(\eta_{i+j},\eta_j)_v(\eta_{i+j},\lambda)_v^{-j}$ *for all* $i,j \geq 1$
2. *if* $i+j \geq p+1$, *then* $(a,b)_v = 1$ *for all* $a \in U_i$ *and* $b \in U_j$
3. $(\eta_i,\lambda)_v = \begin{cases} 1 & \text{if } 1 \leq i \leq p-1 \\ \zeta_p & \text{if } i = p \end{cases}$

Proof. Because $\eta_j + \lambda^j\eta_i = \eta_{i+j}$, we have $1 - \frac{\eta_j}{\eta_{i+j}} = \frac{\lambda^j\eta_i}{\eta_{i+j}}$. Thus

$$\begin{aligned} 1 = \left(\frac{\eta_j}{\eta_{i+j}}, 1-\frac{\eta_j}{\eta_{i+j}}\right)_v &= \left(\frac{\eta_j}{\eta_{i+j}}, \frac{\lambda^j\eta_i}{\eta_{i+j}}\right)_v \\ &= (\eta_j,\lambda^j\eta_i)_v\left(\frac{1}{\eta_{i+j}},\lambda^j\eta_i\right)_v\left(\eta_j,\frac{1}{\eta_{i+j}}\right)_v \\ &= (\eta_j,\eta_i)_v(\lambda,\eta_{i+j})_v^j(\eta_i,\eta_{i+j})_v(\eta_{i+j},\eta_j)_v \end{aligned}$$

and we have proved part 1. Part 2 follows from part 1 and the observation that η_{i+j} is in the trivial class for $i+j \geq p+1$.

The first $p-1$ cases of part 3 are trivial, because $(\eta_i,\lambda)_v^i = (1-\lambda^i,\lambda^i)_v = 1$, thus $(\eta_i,\lambda)_v = 1$ in these cases. For the final case, we observe that if we can show that the extension $K_v(\sqrt[p]{\eta_p})/K_v$ is unramified, then we can use [CF67, Proposition VI.2.5.2] to conclude that $(\eta_p,\lambda)_v = \frac{(\sqrt[p]{\eta_p})^{F^{\mathrm{val}(\lambda)}}}{\sqrt[p]{\eta_p}}$ where F is the Frobenius associated to the extension $K_v(\sqrt[p]{\eta_p})/K_v$. We know that $\mathrm{val}(\lambda) = 1$, thus the desirable result emerges. Let $\eta_p = \alpha^p$, and write $\alpha = 1+\lambda x$. We see that x is a root of the polynomial $f(X)$ such that $f(X) = X^p - X + 1 \pmod{p_v}$. Thus $f'(x) \equiv -1 \neq 0 \pmod{p_v}$, and by [CF67, Proposition 1.7.1], it follows that $K_v(x) = K_v(\alpha)$ is an unramified extension of K_v.

□

From Proposition 3.2.7 we obtain a matrix with entries given as powers of our specified root of unity ζ_p. We instead give a matrix with entries given in $\mathbb{Z}/p\mathbb{Z}$, where ζ_p corresponds to 1. In the $p = 3$ case, we use the following matrix.

	λ	η_1	η_2	η_3
λ	0	0	0	-1
η_1	0	0	1	0
η_2	0	-1	0	0
η_3	1	0	0	0

Table 3.1: Matrix for computing local pairing in $p = 3$ case.

In the $p = 5$ case, we use the following matrix.

	λ	η_1	η_2	η_3	η_4	η_5
λ	0	0	0	0	0	-1
η_1	0	0	-1	1	1	0
η_2	0	1	0	2	0	0
η_3	0	-1	-2	0	0	0
η_4	0	-1	0	0	0	0
η_5	1	0	0	0	0	0

Table 3.2: Matrix for computing local pairing in $p = 5$ case.

3.3 The Pushout Function Definition

The definition of the Cassels-Tate pairing we describe in this section will be the most useful to us, computationally speaking. Let $x, y \in Ш(\hat{E}/K)$ as before, where we have a p-isogeny ϕ.

$$E \xrightarrow{\phi} \hat{E} \xrightarrow{\hat{\phi}} E, \;\; \hat{\phi} \circ \phi = [p]$$

Let $T \in E[\phi]$ and $\hat{T} \in \hat{E}[\hat{\phi}]$ be generators of these groups, and denote by A_2 and A_1 the étale algebras attached to $E[\phi] \setminus \{\mathcal{O}\}$ and $\hat{E}[\hat{\phi}] \setminus \{\mathcal{O}\}$, respectively, as is done in Section 2.3.

We seek to compute the Cassels-Tate pairing $< x, y >_{\mathrm{CT}}$. Once again, we define the Cassels-Tate pairing on these elements only in the case that $\hat{\phi}(y) = 0$. The first ingredient we need for this alternative definition is another local pairing. Recall from Section 2.3 that we have the group homomorphisms

$$\begin{aligned} \overline{w}_{\phi} &: H^1(K, E[\phi]) \longrightarrow A_1^{\times}/(A_1^{\times})^p \\ \overline{w}_{\hat{\phi}} &: H^1(K, \hat{E}[\hat{\phi}]) \longrightarrow {A_2}^{\times}/({A_2}^{\times})^p \end{aligned} \tag{3.10}$$

where

$$\mathrm{im}(\overline{w}_{\phi}) = \ker(g - \sigma_g) \tag{3.11}$$

for g a primitive root mod p and σ_g the corresponding automorphism of A_1.

Let $\eta \in S^{(\hat{\phi})}(\hat{E}/K)$ be an element that maps to y, which exists by the exact sequence (3.2). For every place v of K, we have $A_1 \otimes_K K_v = A_{1,v}$, and the local analogue of (3.10) is a map $\overline{w}_{\phi,v}$ that makes the following diagram commute.

$$\begin{array}{ccc} \overline{w}_{\phi} : H^1(K, E[\phi]) & \hookrightarrow & A_1^{\times}/(A_1^{\times})^p \\ \Big\downarrow \mathrm{Res}_v & & \Big\downarrow \\ \overline{w}_{\phi,v} : H^1(K_v, E[\phi]) & \hookrightarrow & A_{1,v}^{\times}/(A_{1,v}^{\times})^p \end{array}$$

Similarly, a map $\overline{w}_{\hat{\phi},v} : H^1(K, \hat{E}[\hat{\phi}]) \hookrightarrow A_{2,v}^{\times}/(A_{2,v}^{\times})^p$ also exists. Let $[\ ,\ ]_v$ denote the pairing induced by $<\ ,\ >_{v,e_\phi}$ on the images of $\overline{w}_{\phi,v}$ and $\overline{w}_{\hat{\phi},v}$. As in (3.7), this pairing satisfies a product formula

$$\sum_{v \in M_K} [a, b]_v = 0 \text{ for all } a \in \mathrm{im}(\overline{w}_{\phi}) \text{ and } b \in \mathrm{im}(\overline{w}_{\hat{\phi}}). \tag{3.12}$$

Introducing the Pushout Function

For $x \in Ш(\hat{E}/K)$, let C be a torsor under $\hat{E}$ representing x. For each $\mathscr{O} \neq \hat{S} \in \hat{E}[\hat{\phi}]$, let $D_{\hat{S}}$ be a divisor corresponding to $\hat{S}$ under the isomorphism of Galois modules sum: $\mathrm{Pic}^0(C) \cong \hat{E}$. Because C is everywhere locally soluble, by [Cas62, Lemma 7.1] we can choose the divisors $D_{\hat{S}}$ such that the map $\hat{S} \mapsto D_{\hat{S}}$ is Galois equivariant. Since $\mathrm{sum}(p \cdot D_{\hat{S}}) = p \cdot \hat{S} = \mathscr{O}$, we can use Proposition 3.1.2 to conclude that there are rational functions $f_{\hat{S}} \in \overline{K}(C)$ with $\mathrm{div}(f_{\hat{S}}) = p \cdot D_{\hat{S}}$. Using Hilbert's Theorem 90, we can scale the $f_{\hat{S}}$ such that $f = (\hat{S} \mapsto f_{\hat{S}})$. is Galois equivariant. Then f is an element of $A_1(C) = A_1 \otimes_K K(C) = \mathrm{Map}_K(\hat{E}[\hat{\phi}] \setminus \{\mathscr{O}\}, \overline{K}(C))$.

Definition 3.3.1. The function f thus constructed is called a *pushout function for x*.

This definition of the pushout function, together with the definition of the local pairing $[\ ,\ ]_v$ are used in the following definition of the Cassels-Tate pairing. It is a nontrivial task to prove that this definition matches Definition 3.1.6. This will be done in Theorem 3.3.5.

Definition 3.3.2 (Pushout function definition of the Cassels-Tate pairing)**.** For $x \in Ш(\hat{E}/K)$ and $y \in Ш(\hat{E}/K)[\phi]$, the Cassels-Tate pairing can be given by

$$< x, y >= \sum_{v \in M_K} [f(P_v), \overline{w}_{\hat{\phi}}(\eta)]_v$$

where $[\ ,\ ]_v$ is the local pairing induced on $\mathrm{im}\,(\overline{w}_{\phi,v}) \times \mathrm{im}\,(\overline{w}_{\hat{\phi},v})$ by the local Tate pairing $<\ ,\ >_{v,e_\phi}$ from Definition 3.1.4. We let C/K be a torsor under $\hat{E}$ representing x, and define $f = (\hat{S} \mapsto f_{\hat{S}})$ by the construction given above. For each place v of K we choose a local point $P_v \in C(K_v)$ such that the poles and zeroes of the rational functions $f_{\hat{S}}$ are avoided.

The first thing we must show is the following.

Theorem 3.3.3. *Definition 3.3.2 is well-defined.*

The following lemma will help us to prove this theorem.

Lemma 3.3.4. *Let $f \in A_1(C)$ as above. After multiplying f by a suitable element of $A_1^\times$, there exists $r \in A_1(C)$ such that*

$$\frac{\sigma_g(f)}{f^g} = r^p. \tag{3.13}$$

The proof of this lemma is very similar to that of [FN14, Lemma 1.2].

Proof. Since $\mathrm{sum}(D_{gT} - gD_T) = \mathscr{O}$, we can choose $r \in A_1(C)$ satisfying

$$\mathrm{div}(r_T) = D_{gT} - gD_T$$

thus (3.13) holds up to scalars. From Lemma 3.1.5, we have that for $x \in H^1(K, \hat{E})$ there exists some $x_1 \in H^1(K, E)$ such that $\phi(x_1) = x$. Let C and C_1 be the covering curves corresponding to the classes x and x_1 respectively. Then there is a commutative diagram

$$\begin{array}{ccc} C_1 & \xrightarrow{\pi} & C \\ {\scriptstyle \cong/\overline{K}}\downarrow & & \downarrow{\scriptstyle \cong/\overline{K}} \\ E & \xrightarrow{\phi} & \hat{E} \end{array}$$

where π is a morphism defined over K, and the vertical maps are isomorphisms defined over $\overline{K}$. For $\hat{S} \in \hat{E}[\hat{\phi}] \setminus \{\mathscr{O}\}$, there exists $S \in E[p]$ such that $\phi(S) = \hat{S}$. Let B_S be the divisor corresponding to S under the isomorphism of Galois modules sum: $\mathrm{Pic}^0(C_1) \cong E$. Because C_1 is everywhere locally soluble, we can choose the B_S such that the map $S \mapsto B_S$ is Galois equivariant. Then

$$\phi^*(A_{\hat{S}}) = \sum_{P \in E[\phi]} B_{S+P}$$

and $\mathrm{sum}\left(\sum_{P\in E[\phi]} B_{S+P}\right) = \mathscr{O}$, so there exists $\mathscr{F} \in A_1(C_1)$ with $\mathrm{div}(\mathscr{F}_S) = \pi^* D_{\hat{S}}$. We now scale f and r so that

$$\pi^* f = \mathscr{F}^p \qquad \text{and} \qquad \pi^* r = \frac{\sigma_g(\mathscr{F})}{\mathscr{F} g}.$$

The condition (3.13) now follows. □

We can now prove that Definition 3.3.2 is well-defined.

Proof of Theorem 3.3.3. We must show is that $f(P_v)$ is in the image of $\overline{w}_{\phi,v}$ and is therefore a valid argument for $[\ ,\ ]_v$. This follows from Lemma 3.3.4 and the description of $\mathrm{im}(\overline{w}_\phi)$ in (3.11). By [Sha98, Theorem 2.3] evaluating f on degree 0 divisors yields elements in the image of the connecting map $\delta_{\hat{\phi},v}$. As in the proof of Theorem 3.1.7, Tate local duality then gives us that this definition is independent of choice of $P_v \in C(K_v)$. The pairing is also independent of the choice of scaling of f, by the product formula (3.12). □

We would also like to see that this definition which looks a bit different from Definition 3.1.6 is actually the same. The following proof is a slight modification of that in [FN14].

Theorem 3.3.5. *The pushout function definition 3.3.2 and the Weil pairing definition 3.1.6 of the Cassels-Tate pairing are the same.*

Proof. If we have C and C_1 corresponding to classes x and x_1 in $H^1(K,\hat{E})$ and $H^1(K,E)$ respectively, with $\phi(x_1) = x$, then we have a commutative diagram

$$\begin{array}{ccc} C_1 & \xrightarrow{\pi} & C \\ \downarrow & & \downarrow \\ E & \xrightarrow{\phi} & \hat{E} \end{array}$$

where π is a ϕ-covering of C, which is a morphism defined over K. As in the proof of Lemma 3.3.4 we may scale $f \in A_1(C)$ such that $\pi^* f = \mathscr{F}^p$ for some $\mathscr{F} \in A_1(C_1)$. C is everywhere locally soluble, therefore at all places v of K we have a ϕ-covering $\pi_v : C_{1,v} \to C$ defined over K_v with $C_{1,v}(K_v) \neq \emptyset$. In fact, each such π_v is the twist of $\pi : C_1 \to C$ by some $\xi_v \in H^1(K_v, E[\phi])$, and we have $\pi_v^* f = \overline{w}_{\phi,v}(\xi_v)\mathscr{F}_v^p$ with $\mathscr{F}_v \in A_1$. This ξ_v was used in the Weil pairing definition, which said that the pairing was calculated by

$$\sum_{v \in M_K} < \xi_v, b_v >_{v,e_\phi}$$

so what we want to show is that $\overline{w}_\phi(\xi_v) \equiv f(P_v) \bmod (A_{1,v}^\times)^p$ and the proof will be complete.

Let $P_v \in \pi_v(C_{1,v}(K_v))$, not a pole or a zero of f, which must exist because $C_{1,v}(K_v)$ contains infinitely many points. Because π_v is a twist of π, we have the following commutative diagram

$$\begin{array}{ccc} C_{1,v} & \xrightarrow{\pi_v} & C \\ \downarrow{\scriptstyle \psi} & & \| \\ C_1 & \xrightarrow{\pi} & C \end{array}$$

where ψ is an isomorphism defined over $\overline{K}_v$.

We have that ξ_v is represented by a cocycle $(\sigma \mapsto \xi_{\sigma,v})$ where $\psi^\sigma \psi^{-1}$ describes translation by $\xi_{\sigma,v} \in E[\phi]$. Let the following map be induced by the Weil pairing

$$w : E[\phi] \to \mu_p(\overline{A_{1v}}).$$

We have that $\psi^* \mathscr{F} = \gamma \mathscr{F}_v$ for some $\gamma \in \overline{A_{1v}}^\times$. By Definition 3.1.3, we see that

$$w(\xi_{\sigma,v})\mathscr{F} = (\psi^\sigma \psi^{-1})^* \mathscr{F} = \frac{\sigma(\gamma)}{\gamma}\mathscr{F}$$

thus $w(\xi_{\sigma,v}) = \frac{\sigma(\gamma)}{\gamma}$ and so ξ_v can be expressed as $\gamma^p \bmod (A_{1,v}^\times)^p$, as we saw in Section 2.3. We also have $\pi_v^* f = \gamma^p \mathscr{F}_v^p$, from which it follows that $\gamma^p \equiv f(P_v) \bmod (A_{1,v}^\times)^p$, which completes the proof. □

Definition 3.3.2 uses an infinite sum, but only a certain finite set of primes need be considered. The following is an analogue of [FN14, Lemma 1.5]. Denote by $O_v \subset A_{1,v}$ the product of valuation rings of this product of fields, and l_v for the product of residue fields. Let k_v be the residue field for K_v.

Proposition 3.3.6. *Let C/K and $f \in A_1(C)^\times$ be defined as in Definition 3.3.2. If $v \nmid p\infty$ is a prime of good reduction for C, and f reduces modulo v to $\widetilde{f} \in l_v(\widetilde{C})^\times$ then*

$$f(P_v) \in \mathrm{im}(\overline{w}_\phi \circ \delta_{\phi,v})$$

for all $P_v \in C(K_v)$ avoiding the zeroes and poles of the $f_{\hat{S}}$.

By Tate local duality [Ser02, Theorem 2.5.2], it follows from this theorem that the only primes we need to consider are those for which this proposition does not hold, which is a finite set.

Proof. It is sufficient to prove the proposition for just one choice of P_v, by the proof of Theorem 3.3.3.

If the residue k_v is large enough, then there is some $\widetilde{P}_v \in \widetilde{C}(k_v)$ avoiding the zeroes and poles of the $\widetilde{f}_{\hat{S}}$ and we can lift this $\widetilde{P}_v$ to $P_v \in C(K_v)$. We also know that $f(P_v)$ is a unit, thus

$$f(P_v) \in \mathrm{im}(\overline{w}_\phi) \cap O_v^\times / (O_v^\times)^p.$$

We know that $\mathrm{im}(\delta_{\phi,v})$ is the unramified subgroup of $H^1(K_v, E[\phi])$ [SS03, Proposition 3.2], and that $O_v^\times/(O_v^\times)^p$ is the kernel of the map

$$(A_1 \otimes_K K_v)^\times / \{p\text{th powers}\} \longrightarrow (A_1 \otimes_K K_v^{\mathrm{nr}})^\times / \{p\text{th powers}\}.$$

Thus we find $f(P_v) \in \mathrm{im}(\overline{w}_\phi \circ \delta_{\phi,v})$, as required.

Should we find that k_v is too small, we can make an unramified extension of degree coprime to p to sufficiently enlarge it. □

Example 3.3.7. Let E be the Cremona curve 200907b1, and thus given by

$$E : y^2 = x^3 - 3(10x+28)^2.$$

Let $L_1 = \mathbb{Q}(\zeta_3)$, $L_2 = \mathbb{Q}(\beta)$ where $\beta^3 = 1063$. Then we have that the torsion group $E[3] = \langle S, T\rangle$ where

$$S = (0, -56\zeta_3 - 28)$$
$$T = (4/3\beta^2 + 40/3\beta + 400/3, -40/3\beta^2 - 400/3\beta - 4252/3)$$

Let ϕ be the isogeny from $E \to \hat{E}$ where $\hat{E} : y^2 = x^3 + (30x+4252)^2$ with kernel generated by $\langle S\rangle$. Then we have the following Selmer groups.

$$S^{(\phi)}(E/\mathbb{Q}) = \langle 1063\rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^3$$
$$S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) = \langle \zeta_3, -21\zeta_3 - 14\rangle \subset (L_1^\times/(L_1^\times)^3)^-$$

An initial rank estimate would therefore be 2. The generators of $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ can be expressed as covering curves as follows using either Section 2.4 or Section 3.5.

$S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$	covering curve
ζ_3	$x^3 - 3x^2y + 10x^2z - 10xyz + y^3 + 10y^2z + 7z^3 = 0$
$-7\zeta_3 - 21$	$x^3 + 10xy^2 - 10xyz + 10xz^2 - y^3 - 6y^2z + 9yz^2 - z^3 = 0$

For each pushout function f, we have instead found a cubic form f_1 such that $f = \frac{f_1}{x^3}$. We call f_1 a pushout form, and an example of suitable pushout forms is given in the following table. Sections 3.4 and 3.6 will deal with how to compute these forms. They may however be independently checked by seeing that $\frac{f_1}{x^3}$ does indeed lie in the function field of the associated covering curve, and that $\operatorname{div}\left(\frac{f_1}{x^3}\right) = 3\cdot D$ for some divisor D.

$S^{(\hat{\phi})}(\hat{E}/K)$	pushout forms
ζ_3	$3699x^3 - 1392x^2y - 239x^2z + 105xy^2 - 499xyz + 2460xz^2 - 135y^3 - 1049y^2z$ $+1218yz^2 + 11z^3$
$-7\zeta_3 - 21$	$1823x^3 + 5372x^2y - 14017x^2z - 12963xy^2 - 6651xyz + 8178xz^2 + 2272y^3$ $+11634y^2z + 5652yz^2 - 637z^3$

The primes we must consider is the set $\{3, 7, 1063\}$ of bad primes of E, as discussed in Proposition 3.3.6. In this case, the pushout forms contributed one extra prime so the set of primes we must consider is given by

$$P = \{2, 3, 7, 1063\}.$$

We chose the following local points on our covering curves

$S^{(\hat{\phi})}(\hat{E}/K)$	mod 2^4	mod 3^4	mod 7^4	mod 1063^4
ζ_3	$(15:0:1)$	$(46:0:1)$	$(1481:0:1)$	$(403603745881:0:1)$
$-7\zeta_3 - 21$	$(11:0:1)$	$(56:0:1)$	$(1396:0:1)$	$(811757475299:0:1)$

We thus find $f(P_v) \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^3$ for $p \in P$. Section 3.2 and Definition 3.3.2 can now be used. By filling in these points in the pushout forms, we obtain the following elements.

$S^{(\hat{\phi})}(\hat{E}/K)$	mod 2^4	mod 3^4	mod 7^4	mod 1063^4
ζ_3	13	27	1431	976506231161
$-7\zeta_3-21$	13	20	123	1105975650698

We now use the theory in Section 3.2 to compute the local pairings. The prime 2 is inert in L_1, the primes 7 and 1063 split. In all three cases, we will use part 6 of Proposition 3.2.6 to compute the pairing. The following table gives the necessary information for the prime 2.

$(a,b)_2$	$\mathrm{val}_2(a)$	$\mathrm{val}_2(b)$	c	$\left(\frac{c}{2}\right)$
$(\zeta_3,13)_2$	0	0	1	0
$(-7\zeta_3-21,13)_2$	0	0	1	0

Thus the local pairing in this case is represented by the zero matrix.

Because both of the primes 7 and 1063 split in L_1, we first choose one prime lying over each one. Thus we find the prime $p_7 = 3\zeta_3+1$ lying over 7 and $p_{1063} = -3\zeta_3-34$ lying over 1063. The following tables give us the necessary information for these primes.

$(a,b)_{p_7}$	$\mathrm{val}_{p_7}(a)$	$\mathrm{val}_{p_7}(b)$	c	$\left(\frac{c}{p_7}\right)$
$(\zeta_3,1431)_{p_7}$	0	0	1	0
$(\zeta_3,123)_{p_7}$	0	0	1	0
$(-7\zeta_3-21,1431)_{p_7}$	1	0	$\frac{1}{1431}$	2
$(-7\zeta_3-21,123)_{p_7}$	1	0	$\frac{1}{123}$	2

$(a,b)_{p_{1063}}$	$\mathrm{val}_{p_{1063}}(a)$	$\mathrm{val}_{p_{1063}}(b)$	c	$\left(\frac{c}{p_{1063}}\right)$
$(\zeta_3,976506231161)_{p_{1063}}$	0	0	1	0
$(\zeta_3,1105975650698)_{p_{1063}}$	0	1	ζ_3	0
$(-7\zeta_3-21,976506231161)_{p_{1063}}$	0	0	1	0
$(-7\zeta_3-21,1105975650698)_{p_{1063}}$	0	1	$-7\zeta_3-21$	0

The local pairing in both these cases is obtained by multiplying the pairings in the table by 2, as described by Remark 3.2.4. Thus we obtain the following matrices for these local pairings.

$\mathbb{Q}_7$	ζ_3	$-7\zeta_3-21$
ζ_3	0	0
$-7\zeta_3-21$	1	1

$\mathbb{Q}_{1063}$	ζ_3	$-7\zeta_3-21$
ζ_3	0	0
$-7\zeta_3-21$	0	0

We now move on to the final prime, 3, which is completely ramified in L_1. We must use Proposition 3.2.7 to compute this local pairing. Each of the elements being used lies in one of the classes generated by $\langle\lambda,\eta_1,\eta_2,\eta_3\rangle$. The following table indicates which class each element is in.

element	class	element	class
ζ_3	η_1	27	1
$-7\zeta_3-21$	$\eta_1\eta_3$	20	$\eta_2^2\eta_3^2$

Using Table 3.1 we thus obtain the following matrix for the local pairing at 3.

$\mathbb{Q}_3$	ζ_3	$-7\zeta_3-21$
ζ_3	0	2
$-7\zeta_3-21$	0	2

We add together the four matrices of the local pairings to obtain the following matrix for the Cassels-Tate pairing.

$<,>_{CT}$	ζ_3	$-7\zeta_3-21$
ζ_3	0	2
$-7\zeta_3-21$	1	0

Thus we see that $\text{rank}(E(\mathbb{Q}))=0$ and $Ш(\hat{E}/\mathbb{Q})[\hat{\phi}] \cong (\mathbb{Z}/3\mathbb{Z})^2$.

3.4 Computing the Pushout Function

In the previous section, we encountered the pushout function definition of the Cassels-Tate pairing. This definition will be used in the calculations in Chapters 5-8 of this thesis, therefore in this section and the next we will show how to calculate such pushout functions.

First we recall the definition of a pushout function. Let $E \xrightarrow{\phi} \hat{E}$ be an n-isogeny as usual, for some integer n. Let $x \in S^{(\hat{\phi})}(\hat{E}/K)$ be represented as a $\hat{\phi}$-covering curve C of E. As we saw before, $E[\phi]$ is cyclic therefore we let T be a generator for it and A a divisor on C of degree 0 whose class maps to T under the isomorphism sum: $\text{Pic}^0(C) \cong E$. Then a pushout function f is a rational function on C with $\text{div}(f) = n \cdot A$. In practice, we have C given as a curve in $\mathbb{P}^{n^2-1}$, and we find a degree n form f_1 in some variables $x_1,\ldots,x_n$ with $f = \frac{f_1}{x_1^n}$. This form f_1 is what we have called a *pushout form*. Of course, it makes no difference whether we use the pushout form or the pushout function in Definition 3.3.2.

Consider some $x \in S^{(\hat{\phi})}(\hat{E}/K)$ given as some $\hat{\phi}$-covering curve C of E. The first step in computing a pushout form is to lift x to some element of $H^1(K,E[n])$, as is explored in Section 2.5. This lift requires the solving of a norm equation, as is explained in Section 2.5. This is potentially a very computationally heavy step to take, which is why Chapter 4 deals separately with the issue.

In what follows in this section, we are working towards a concrete realisation of the elements of $H^1(K,E[n])$, given in Definition 3.4.1. We then build towards Proposition 3.4.11, which is a very useful tool in calculating the pushout forms we need. We follow a series of three papers [CFO+08, CFO+09, CFO+12].

3.4.1 Two Concrete Realisations of $H^1(K,E[n])$

Let R be the Galois equivariant maps from $E[n]$ to $\overline{K}$.

$$R = \text{Maps}_K(E[n],\overline{K})$$

In fact, as in Section 2.3, R is an étale algebra isomorphic to the product

$$R \cong L_1 \times \ldots \times L_t$$

where each L_i represents a G_K-orbit in $E[n]$. We will also use $\overline{R} = R \otimes_K \overline{K} = \text{Maps}(E[n], \overline{K})$.

The Weil pairing $e_n : E[n] \times E[n] \to \mu_n$ gives us an injection

$$w : E[n](\overline{K}) \hookrightarrow \overline{R}^\times = \text{Map}(E[n](\overline{K}), \overline{K}^\times). \tag{3.14}$$

Thus for every $T \in E[n]$, we obtain a homomorphism $w(T) : E[n] \to \overline{K}^\times$. We now define $\partial : \overline{R}^\times \to (\overline{R} \otimes_{\overline{K}} \overline{R})^\times$ by setting

$$(\partial\alpha)(T_1, T_2) = \frac{\alpha(T_1)\alpha(T_2)}{\alpha(T_1 + T_2)}. \tag{3.15}$$

We take Galois cohomology of the following exact sequence

$$0 \to E[n] \xrightarrow{w} \overline{R}^\times \xrightarrow{\partial} \partial\overline{R}^\times \to 0 \tag{3.16}$$

to obtain

$$0 \to E(K)[n] \xrightarrow{w} R^\times \to (\partial\overline{R}^\times)^{G_K} \to H^1(K, E[n]) \to H^1(K, \overline{R}^\times)$$

and by Hilbert's Theorem 90, the last group in this sequence is trivial, thus we obtain an isomorphism

$$H^1(K, E[n]) \cong (\partial\overline{R}^\times)^{G_K} / \partial R^\times. \tag{3.17}$$

We can now define two group homomorphisms.

Definition 3.4.1. Let $\xi \in H^1(K, E[n])$, then by Hilbert's Theorem 90 there exists some $\gamma \in \overline{R}^\times$ such that $w(\xi_\sigma) = \frac{\sigma(\gamma)}{\gamma}$. Then we define

$$w_1 : H^1(K, E[n]) \longrightarrow \frac{R^\times}{(R^\times)^n}$$
$$w_2 : H^1(K, E[n]) \longrightarrow \frac{(R \otimes R)^\times}{\partial R^\times}$$

with

$$w_1(\xi) = \alpha \pmod{(R^\times)^n} \qquad \text{where } \alpha = \gamma^n \tag{3.18}$$
$$w_2(\xi) = \rho \pmod{\partial R^\times} \qquad \text{where } \rho = \partial\gamma. \tag{3.19}$$

The map w_1 is in fact the composite of the two maps

$$H^1(K, E[n]) \xrightarrow{w_*} H^1(K, \mu_n(\overline{R})) \xrightarrow{\kappa} R^\times / (R^\times)^n$$

where w_* is induced by the map w from (3.14) and κ is the Kummer isomorphism. Before proceeding, we must show the following.

Lemma 3.4.2. *Definition 3.4.1 is well defined.*

Proof. We first note that $\alpha = \gamma^n$ and $\rho = \partial\gamma$ are Galois invariant, and therefore belong to $R^\times$ and $(R\otimes R)^\times$ respectively. If we make a different choice for ξ, say ξ', then ξ' differs from ξ by some coboundary, say $\sigma \mapsto \sigma(T) - T$. Then we find $\gamma' = \gamma w(T)$. Because $w(T)^n = 1$ and $\partial(w(T)) = 1$, we have $w_1(\xi) = w_1(\xi')$ and $w_2(\xi) = w_2(\xi')$. If we multiply γ by an element of $R^\times$, the effect is to multiply α and ρ by elements in $(R^\times)^n$ and $\partial R^\times$, respectively. Thus w_1 and w_2 are well defined. □

The homomorphisms in Definition 3.4.1 have the following important property.

Lemma 3.4.3. *The homomorphism w_2 from Definition 3.4.1 is injective, and the homomorphism w_1 is injective in the case that n is prime.*

Proof. We know that w_1 is injective for prime n by Proposition 2.3.5. In general, w_1 is not injective. Because w_2 consists simply of the isomorphism (3.17) composed with the natural inclusion $(\partial\overline{R}^\times)^{G_K}/\partial R^\times \hookrightarrow (R\otimes R)^\times/\partial R^\times$, we know that w_2 is also injective. □

Using Definition 3.4.1, we can express $\xi \in S^{(n)}(E/K)$ as either some $\alpha \in R^\times/(R^\times)^n$ or some $\rho \in (R\otimes R)^\times/\partial R^\times$. Usually, we will have it in the form α. To compute a pushout form, we will be using Proposition 3.4.11, which uses the form ρ. Therefore, given α, we want to be able to calculate a suitable ρ. We can extend sequence (3.16) to the complex

$$0 \to E[n] \xrightarrow{w} \overline{R}^\times \xrightarrow{\partial} (\overline{R}\otimes\overline{R})^\times \xrightarrow{\Delta} (\overline{R}\otimes\overline{R}\otimes\overline{R})^\times \tag{3.20}$$

where Δ is given by

$$(\Delta\rho)(T_1,T_2,T_3) = \frac{\rho(T_1,T_2)\rho(T_1+T_2,T_3)}{\rho(T_1,T_2+T_3)\rho(T_2,T_3)}.$$

Then the following lemma gives a characterisation of the image of w_2.

Notation 3.4.4. *Let* $\mathrm{Sym}^2_K(R)$ *denote the subalgebra of symmetric functions*

$$\mathrm{Sym}^2_K(R) = \{\rho \in R\otimes_K R \mid \rho(T_1,T_2) = \rho(T_2,T_1) \text{ for all } T_1,T_2 \in E[n]\}$$

Lemma 3.4.5 ([CFO+08, Lemma 3.5])**.** *The image of w_2 is*

$$\mathrm{im}(w_2) = \left\{\rho \in \mathrm{Sym}^2_K(R)^\times \mid \Delta\rho = 1\right\}/\partial R^\times$$

It also follows that for any $\rho \in \mathrm{im}(w_2)$ that $\rho = \partial\gamma$ for some $\gamma \in \overline{R}^\times$.

We refer to [CFO+08] for the proof of this lemma. The following lemma follows from the definitions and tells us how to compute ρ from α.

Lemma 3.4.6 ([CFO+08, Lemma 3.8])**.** *Let $\alpha(R^\times)^n$ belong to the image of w_1. Then there exists $\rho \in \mathrm{Sym}^2(R)^\times$ with*

1. $\partial\alpha = \rho^n$,
2. $\alpha(T) = \prod_{i=0}^{n-1}\rho(T,iT)$ *for all* $T \in E[n]$,
3. $\Delta\rho = 1$.

Moreover, if $\rho \in \mathrm{Sym}^2_K(R)^\times$ satisfies conditions 2 and 3, then ρ corresponds to α.

Proof. Let γ be such that $\gamma(T)^n = \alpha(T)$ for $T \in E[n]$, and let

$$\rho(T_1,T_2) = \frac{\gamma(T_1)\gamma(T_2)}{\gamma(T_1+T_2)}. \tag{3.21}$$

Then we have

$$\begin{aligned}\rho(T_1,T_2)^n &= \frac{\gamma(T_1)^n\gamma(T_2)^n}{\gamma(T_1+T_2)^n} = \frac{\alpha(T_1)\alpha(T_2)}{\alpha(T_1+T_2)} \\ &= \partial\alpha(T_1,T_2)\end{aligned}$$

and

$$\begin{aligned}\prod_{i=0}^{n-1}\rho(T,iT) &= \frac{\gamma(T)^n\gamma(\mathscr{O})\gamma(T)\cdots\gamma((n-1)T)}{\gamma(\mathscr{O})\gamma(T)\cdots\gamma((n-1)T)} \\ &= \alpha(T)\end{aligned}$$

proving conditions 1 and 2. We also have

$$\begin{aligned}(\Delta\rho)(T_1,T_2,T_3) &= \frac{\gamma(T_1)\gamma(T_2)\gamma(T_1+T_2)\gamma(T_3)\gamma(T_1+T_2+T_3)\gamma(T_2+T_3)}{\gamma(T_1+T_2)\gamma(T_1+T_2+T_3)\gamma(T_1)\gamma(T_2+T_3)\gamma(T_2)\gamma(T_3)} \\ &= 1\end{aligned}$$

proving condition 3. Conversely, if $\rho \in \mathrm{Sym}^2_K(R)^\times$ satisfies conditions 2 and 3, then by Lemma 3.4.5 it lies in the image of w_2 and so there exists some $\gamma \in \overline{R}^\times$ with $\rho = \partial\gamma$. It follows from condition 2 that $\alpha = \gamma^n$. □

If $\mathrm{Sym}^2_K(R)$ contains no nontrivial nth roots of unity, then it is very easy to compute ρ from α. We simply let ρ be the unique nth root of $\partial\alpha$. In other cases, some choice is involved. The first thing we want to know is how much choice we have. Let Γ be the set of all maps $\gamma : E[n] \to \mu_n$ satisfying

$$\frac{\gamma(\sigma T_1)\gamma(\sigma T_2)}{\gamma(\sigma(T_1+T_2))} = \sigma\left(\frac{\gamma(T_1)\gamma(T_2)}{\gamma(T_1+T_2)}\right)$$

for all $\sigma \in G_K$ and $T_1, T_2 \in E[n]$. Then, from the Weil pairing (compare (3.16)) we obtain an exact sequence of G_K-modules

$$0 \to E[n] \xrightarrow{w} \Gamma \xrightarrow{\partial} \partial\Gamma \to 0.$$

Lemma 3.4.7. *The image of ∂ is given by*

$$\partial\Gamma = \left\{\rho \in \mathrm{im}(w_2) \mid \prod_{i=0}^{n-1}\rho(T,iT) = 1 \text{ for all } T \in E[n]\right\}.$$

Proof. By Lemma 3.4.5 every $\rho \in \mathrm{im}(w_2)$ can be written as $\rho = \partial\gamma$ for some $\gamma \in \overline{R}^\times$. It therefore follows that $\prod_{i=0}^{n-1}\rho(T,iT) = \gamma(T)^n$, which is 1 in this case. □

Given some $\alpha \in R^\times$ in the image of w_1, we want to find some $\rho \in \mathrm{im}(w_2)$ such that $\Delta\rho = 1$. The number of such ρ is $\#(\partial\Gamma) = \frac{\#\Gamma}{n^2}$. Thus to compute a ρ from an α, we proceed as follows. First we find all nth roots of $\partial\alpha$ in $\mathrm{Sym}^2_K(R)$. Then, we use conditions 2 and 3 of Lemma 3.4.6 to reduce the size of this set until there are only $\#(\partial\Gamma)$ choices left. Every ρ in this set satisfies conditions 2 and 3 of that lemma, and we can choose any one of them. In Section 8.1, we show how to calculate ρ in the case of an elliptic curve E having a rational 5-torsion point.

3.4.2 Method for Computing the Pushout Form

In this section, we will consider $\xi \in H^1(K, E[n])$ as a geometric object. Recall from Definition 3.4.1 that we already have two concrete expressions for ξ given by

$$w_1(\xi) = \alpha \in \frac{R^\times}{(R^\times)^n} \qquad\qquad w_2(\xi) = \rho \in \frac{(R \times R)^\times}{\partial R^\times}. \tag{3.22}$$

These expressions for ξ will occur throughout this section, and we can move freely between them.

Let $e_n : E[n] \times E[n] \to \mu_n$ be the Weil pairing, and let $T_i \in E[n](\overline{K})$. By Proposition 3.1.2 there exists a rational function $G_{T_i} \in \overline{K}(E)^\times$ with divisor

$$\operatorname{div}(G_{T_i}) = [n^*](T_i) - [n^*](\mathscr{O}) = \sum_{n \cdot P = T_i} (P) - \sum_{n \cdot Q = \mathscr{O}} (Q)$$

and the property that $G_{T_i}(P + T_j) = e_n(T_j, T_i) G_{T_i}(P)$ for all $T_i, T_j \in E[n]$ and $P \in E$, as long as both sides are defined. We can make the choice such that $G : T_i \to G_{T_i}$ is Galois equivariant, and interpret G as an element of $R(E)^\times = \operatorname{Map}_K(E[n], \overline{K}(E)^\times)$.

By Proposition 3.1.2, there also exists for every $T_i \in E[n](\overline{K})$ a rational function $F_{T_i} \in \overline{K}(E)^\times$ with

$$\operatorname{div}(F_{T_i}) = n(T_i) - n(\mathscr{O}).$$

By comparing divisors, we see that we can scale F_{T_i} so that $F_{T_i} \circ [n] = G_{T_i}^n$. We can now define $F \in R(E)^\times = \operatorname{Map}_K(E[n], \overline{K}(E)^\times)$ as $F : T_i \mapsto F_{T_i}$, a Galois invariant map. Then F induces a well-defined maps

$$\begin{aligned} F : E(K) \setminus E[n] &\to R^\times / (R^\times)^n \\ P &\mapsto (F_{T_1}(P), \ldots, F_{T_j}(P)) \end{aligned}$$

for $T_1, \ldots, T_j$ representatives of the orbits of $E[n]$ under the action of the Galois group G_K. We can extend F to divisors on E with support disjoing from $E[n]$ by defining

$$F\left(\sum_P n_P (P)\right) = \prod_P F(P)^{n_P}.$$

Then for a principal divisor $A = \operatorname{div}(h)$ we find by Weil reciprocity

$$\begin{aligned} F_{T_i}(A) = F_{T_i}(\operatorname{div}(h)) &= h(\operatorname{div}(F_{T_i})) \\ &= \frac{h(T_i)^n}{h(\mathscr{O})^n} \end{aligned}$$

and so $F(\operatorname{div}(h)) \in (R^\times)^n$. We then obtain the well-defined homomorphism

$$\widetilde{F} : E(\overline{K}) \cong \operatorname{Pic}^0(E/K) \to R^\times / (R^\times)^n. \tag{3.23}$$

Let δ be the connecting homomorphism obtained by taking Galois cohomology of

$$0 \to E[n] \to E \xrightarrow{[n]} E \to 0$$

giving

$$\ldots \to E(K) \xrightarrow{\delta} H^1(K, E[n]) \to H^1(K, E) \to \ldots$$

By [CFO+08, Remark 1.15] $\delta(P)$ is given by the n-covering $(E, t_P \circ [n])$, where t_P is the translation-by-P map.

Proposition 3.4.8. *Recall the map w_1 from Definition 3.4.1. Then the composition $w_1 \circ \delta : E(K) \to R^\times/(R^\times)^n$ is given by $\widetilde{F}$ from* (3.23)*.*

This is a very well-known fact and we refer to [CFO+12, Proposition 2.3] for proof. The following corollary will be useful to us in later calculations.

Corollary 3.4.9. *Let $n = 3$, and let $E[3] = \langle S, T \rangle$. Then the tangents at S and T have divisors $3(S) - 3(\mathscr{O})$ and $3(T) - 3(\mathscr{O})$, respectively, and can therefore be used in the evaluation of the map $\widetilde{F}$.*

Proof. In Section 2.4, we saw that we can write $E : y^2 = x^3 + \Delta(\varepsilon x + \eta)^2$ with $S = \left(0, \eta\sqrt{\Delta}\right)$ and $T = \left(\beta, \frac{\sqrt{\Delta}(\varepsilon\beta+3\eta)}{\sqrt{-3}}\right)$ for β the root of the cubic $\psi(x) = 3x^3 + 4\varepsilon^2\Delta x^2 + 12\varepsilon\eta\Delta x + 12\eta^2\Delta$. The tangent at S is given by

$$L : y - \varepsilon\sqrt{\Delta}x - \eta\sqrt{\Delta} = 0$$

Homogenizing and using the equation for E, we see that we have

$$\frac{Y - \varepsilon\sqrt{\Delta}X - \eta\sqrt{\Delta}Z}{Z} = \frac{X^3}{(Y + \varepsilon\sqrt{\Delta} + \eta\sqrt{\Delta}Z)Z^2}.$$

Because neither Z nor $Y + \varepsilon\sqrt{\Delta} + \eta\sqrt{\Delta}Z$ vanish at S, we see that L has a triple zero at S. We also have that the ideal $M_{\mathscr{O}}$ of functions vanishing at $\mathscr{O}$ is generated by X and Z where $\mathrm{ord}_{\mathscr{O}}(X) = 1$ and $\mathrm{ord}_{\mathscr{O}}(Z) = 3$, thus L has a pole of order 3 at $\mathscr{O}$. We therefore have $\mathrm{div}(L) = 3(S) - 3(\mathscr{O})$, as required. A similar argument, but more complicated, can be made for T, which we omit here. □

We now move on to the actual calculation we want to do in this section. Consider $\xi \in H^1(K, E[n])$ and its associated representatives α and ρ given in (3.22). Let the associated twist of the trivial n-covering $[n] : E \to E$ be given by π. The n-covering $\pi : D \to E$ represents an element of $S^{(n)}(E/K)$ if and only if D is everywhere locally soluble. In [CFO+09], equations for D are found by embedding $D \hookrightarrow \mathbb{P}^{n^2-1}$. To do this, we first write $\mathbb{P}(R)$ for the projective space associated to the K-vector space R. Thus $\mathbb{P}(R) = \mathrm{Proj}(K[R])$ where $K[R] = \otimes_{d\geq 0}\mathrm{Sym}^d(R^*)$ for R^* the dual of R, is the ring of polynomial functions on R. We also define $\mathscr{R} = \mathrm{Spec}(K[R])$, the spectrum of $K[R]$. Define also the following rational function.

$$r_{(T_1,T_2)}(P) = \begin{cases} 1 & \text{if } T_1 = \mathscr{O} \text{ or } T_2 = \mathscr{O} \\ x(P) - x(T_1) & \text{if } T_1 + T_2 = \mathscr{O} \text{ and } T_1 \neq \mathscr{O} \\ \frac{y(P)+y(T_1+T_2)}{x(P)-x(T_1+T_2)} - \lambda(T_1, T_2) & \text{otherwise.} \end{cases} \tag{3.24}$$

The following proposition defines some rational functions $G_{Ti,D}$ in a very similar way to how we defined G_{T_i} earlier.

Proposition 3.4.10 ([CFO+09, Proposition 3.5])**.** *Given D and ρ as above, there are rational functions $G_{T_i,D} \in \overline{K}(D)$, indexed by $T_i \in E[n](\overline{K})$, such that*

1. *The divisor of $G_{T_i,D}$ is*

$$\mathrm{div}(G_{T_i,D}) = \sum_{\pi(P)=T_i} (P) - \sum_{\pi(Q)=\mathscr{O}} (Q) = \pi^*(T_i) - \pi^*(\mathscr{O}).$$

2. *The map $T_i \mapsto G_{T_i,D}$ is G_K-equivariant.*

3. *The functions $G_{T_i,D}$ are scaled so that*

$$r_{(T_1,T_2)}(\pi(P)) = \rho(T_1,T_2)\frac{G_{T_1}(P)G_{T_2}(P)}{G_{T_1+T_2}(P)}.$$

We denote by z_T the coordinate function on $\mathscr{R} \times_{\mathrm{Spec}(K)} \mathrm{Spec}(K(T))$ given by evaluating at T, thus $z_T(\alpha) = \alpha(T)$ for $\alpha \in R$. Over $L = K(E[n])$, these coordinate functions are defined. The z_T can now be used as a set of coordinates on $\mathbb{P}(R)$. We also fix a Weierstrass equation for E, and by $\lambda(T_1,T_2)$ we denote the slope of the line between the points T_1 and T_2 (the tangent line if $T_1 = T_2$).

From part 3 of Proposition 3.4.10 we obtain the relation

$$r_{(T_1,T_2)}(\pi(P))z_{\mathscr{O}}z_{T_1+T_2} = \rho(T_1,T_2)z_{T_1}z_{T_2}. \tag{3.25}$$

The desired embedding is now obtained by forming the scheme maps

$$g_D : D \to \mathbb{P}(R) \cong \mathbb{P}^{n^2-1}$$

by sending $P \in D(\overline{K})$ to the class of the map $(T_i \mapsto G_{T_i}(P))$. The following proposition gives us the equations we are looking for. The quadrics mentioned in it are formed of differences between relations (3.25).

Proposition 3.4.11 ([CFO+09, Proposition 3.7])**.** *Given a Weierstrass equation for E and an element $\rho \in H^1(K,E[n])$, with corresponding n-covering $\pi : D \to E$, we can explicitly compute a set of $n^2(n^2-3)/3$ linearly independent quadrics over K which define the image of*

$$g_D : D \to \mathbb{P}(R) \cong \mathbb{P}^{n^2-1}$$

Enlarging K if necessary to ensure that $E[n](\overline{K}) = E[n](K)$, the z_T are coordinate functions on R, and the defining quadrics can be split into two groups as follows. For all $T_1,T_2 \in E[n](\overline{K}) \setminus \{\mathscr{O}\}$, we have

$$(x(T_1)-x(T_2))z_{\mathscr{O}}^2 + \rho(T_1,-T_1)z_{T_1}z_{-T_1} - \rho(T_2,-T_2)z_{T_2}z_{-T_2} = 0$$

and for all $T_{11},T_{12},T_{21},T_{22} \in E[n](\overline{K}) \setminus \{\mathscr{O}\}$ such that

$$T_{11}+T_{12} = T_{21}+T_{22} = T \neq \mathscr{O},$$

we have

$$(\lambda(T_{21},T_{22}) - \lambda(T_{11},T_{12}))z_{\mathscr{O}}z_T - \rho(T_{11},T_{12})z_{T_{11}}z_{T_{12}} + \rho(T_{21},T_{22})z_{T_{21}}z_{T_{22}} = 0$$

Denote by I_D the ideal generated by the quadrics in this proposition.

We can now show how to use Proposition 3.4.11 to construct pushout forms for the elements of $S^{(\hat{\phi})}(\hat{E}/K)$. Taking Galois cohomology of

$$0 \longrightarrow E[\phi] \longrightarrow E[n] \xrightarrow{\phi} \hat{E}[\hat{\phi}] \longrightarrow 0$$

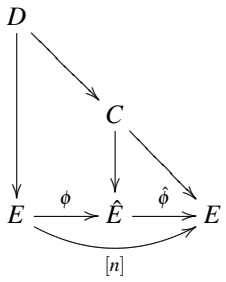
we obtain

$$\hat{E}(K)[\hat{\phi}] \longrightarrow H^1(K,E[\phi]) \longrightarrow H^1(K,E[n]) \longrightarrow H^1(K,\hat{E}[\hat{\phi}])$$

which becomes, when we consider Selmer groups

$$\hat{E}(K)[\hat{\phi}] \longrightarrow S^{(\phi)}(E/K) \longrightarrow S^{(n)}(E/K) \longrightarrow S^{(\hat{\phi})}(\hat{E}/K).$$

Thus given $\xi \in S^{(n)}(E/K)$ and its associated n-covering D, there exists some element $\eta \in S^{(\hat{\phi})}(\hat{E}/K)$ and its associated $\hat{\phi}$-covering C, through which the map $D \to E$ factors.



Assume now that $n = p$, a prime, and let $E[p]$ be generated by S and T such that the kernel $E[\phi]$ is generated by S. Then C can be obtained by quotienting out D by the translation-by-S map μ_S. The function $G_{T_i,D}$ in Proposition 3.4.10 can be seen as the function g in the definition of the Weil pairing in (3.1). Thus for any point $P \in D(\overline{K})$,

$$\frac{G_{T_i,D}(\mu_S(P))}{G_{T_i,D}(P)} = e_p(T_i, S).$$

The only $G_{T_i,D}$ that are invariant under the action of μ_S are therefore those where $T_i = mS$ for $m \in \{0, \ldots, p-1\}$. Thus C is given by the generators of the ideal I_D from Proposition 3.4.11 with all terms except those involving $z_{\mathcal{O}}, z_S, \ldots z_{(p-1)S}$ eliminated. We shall denote the ideal obtained thus by I_C.

We now want to find a pushout form on C. By the construction of the Weil pairing in Section 3.1, if we can find a Kummer generator for the function field extension $\overline{K}(D)/\overline{K}(C)$, then this generator will have all the properties we are looking for. Thus we are seeking a linear form g such that g does not lie in the eigenspace invariant under the action of μ_S, but g^p does. Also we want g to be invariant under the action of the Galois group elements associated to μ_S. If we let

$$g = \sigma_0(a)z_T + \sigma_1(a)z_{S+T} + \ldots + \sigma_{p-1}(a)z_{(p-1)S+T}$$

with a any element and σ_i elements of the Galois group such that $\sigma_i(T) = iS + T$, then g has all the properties we just described and g^p gives a pushout form. By choosing a anything we like we can now express g^p in terms of $z_{\mathcal{O}}, z_S, \ldots z_{(p-1)S}$ using the quadrics that make up the generators of the ideal I_D. We have always chosen $a = 1$ in this thesis as we could find no other element that gave better pushout forms. The cases $p = 3$ and $p = 5$ are calculated in Sections 3.5 and 8.2, respectively.

3.5 The Pushout Form in the General 3-Isogeny Case

In this section, we consider computing the pushout form in the general case that an elliptic curve E admits a 3-isogeny. We use the method outlined in the previous section. As in Section 2.4, let E be given by

$$E : y^2 = x^3 + \Delta(\varepsilon x + \eta)^2. \tag{3.26}$$

The points of order dividing 3 are generated by $E[3] = \langle S, T \rangle$ where

$$S = (0, \eta\sqrt{\Delta})$$
$$T = \left(\beta, \frac{\sqrt{\Delta}(\varepsilon\beta + 3\eta)}{\sqrt{-3}}\right)$$

and β is a root of

$$f(x) = x^3 + \frac{4}{3}\varepsilon^2\Delta x^2 + 4\varepsilon\eta\Delta x + 4\eta^2\Delta.$$

Let G be the subgroup of $GL_2(\mathbb{Z}/3\mathbb{Z})$ through which the action of G_K on $E[3]$ factors. We consider only the case that f is irreducible here, therefore we restrict ourselves to the cases that E is of type generic 3-isogeny, $\mathbb{Z}/3\mathbb{Z}$-nonsplit or μ_3-nonsplit (see Section 2.5). Let σ be such that it permutes the roots of f and $\sigma(T) = S + T$. We label the points of $E[3]$ as follows. For computational reasons we choose that inverses should be numbered with consecutive numbers.

$$T_0 = \mathcal{O}$$
$$T_1 = S = (0, \eta\sqrt{\Delta}) \qquad T_5 = -S + T = (\sigma^2(\beta), \frac{\sqrt{\Delta}(\varepsilon\sigma^2(\beta) + 3\eta)}{\sqrt{-3}})$$
$$T_2 = -S = (0, -\eta\sqrt{\Delta}) \qquad T_6 = S - T = (\sigma^2(\beta), -\frac{\sqrt{\Delta}(\varepsilon\sigma^2(\beta) + 3\eta)}{\sqrt{-3}})$$
$$T_3 = T = (\beta, \frac{\sqrt{\Delta}(\varepsilon\beta + 3\eta)}{\sqrt{-3}}) \qquad T_7 = S + T = (\sigma(\beta), \frac{\sqrt{\Delta}(\varepsilon\sigma(\beta) + 3\eta)}{\sqrt{-3}})$$
$$T_4 = -T = (\beta, -\frac{\sqrt{\Delta}(\varepsilon\beta + 3\eta)}{\sqrt{-3}}) \qquad T_8 = -S - T = (\sigma(\beta), -\frac{\sqrt{\Delta}(\varepsilon\sigma(\beta) + 3\eta)}{\sqrt{-3}})$$

Let $\lambda(T_i, T_j)$ be the slope of the line between T_i and T_j, with $\lambda(T_i, T_i)$ the slope of the tangent line at T_i. Let such a tangent line be given by $y = \lambda(T_i, T_i)x + c_i$. The various λ's and c_i's can easily be computed and depend on ε, η, Δ and β.

Let R be the étale algebra corresponding to $E[3] \setminus \{\mathcal{O}\}$. Let $x \in H^1(K, E[3])$ be represented by $\alpha \in R^\times/(R^\times)^3$ and by $\rho \in (R \otimes R)^\times/\partial R^\times$, as explained in Definition 3.4.1. Recall that there exists $\gamma \in \overline{R}^\times$ such that $\alpha = \gamma^3$ and $\rho = \partial\gamma$. The ideal from Proposition 3.4.11 is generated by the following 27 quadrics. To ease notation, let $\lambda_{ij} = \lambda(T_i, T_j)$, the slope between two points, $\alpha_i = \alpha(T_i)$, $\gamma_i = \gamma(T_i)$, and

$\rho_{i,j} = \rho(T_i, T_j)$ as defined in Section 3.4. We also let $z_{T_i} = z_i$.

$$\beta z_0^2 + \rho_{34} z_3 z_4 - \rho_{12} z_1 z_2 \tag{3.27}$$
$$\sigma^2(\beta) z_0^2 + \rho_{56} z_5 z_6 - \rho_{12} z_1 z_2 \tag{3.28}$$
$$\sigma(\beta) z_0^2 + \rho_{78} z_7 z_8 - \rho_{12} z_1 z_2 \tag{3.29}$$
$$(\lambda_{36} - \lambda_{22}) z_0 z_1 - \rho_{22} z_2^2 + \rho_{36} z_3 z_6 \tag{3.30}$$
$$(\lambda_{47} - \lambda_{22}) z_0 z_1 - \rho_{22} z_2^2 + \rho_{47} z_4 z_7 \tag{3.31}$$
$$(\lambda_{58} - \lambda_{22}) z_0 z_1 - \rho_{22} z_2^2 + \rho_{58} z_5 z_8 \tag{3.32}$$
$$(\lambda_{38} - \lambda_{11}) z_0 z_2 - \rho_{11} z_1^2 + \rho_{38} z_3 z_8 \tag{3.33}$$
$$(\lambda_{45} - \lambda_{11}) z_0 z_2 - \rho_{11} z_1^2 + \rho_{45} z_4 z_5 \tag{3.34}$$
$$(\lambda_{67} - \lambda_{11}) z_0 z_2 - \rho_{11} z_1^2 + \rho_{67} z_6 z_7 \tag{3.35}$$
$$(\lambda_{15} - \lambda_{44}) z_0 z_3 - \rho_{44} z_4^2 + \rho_{15} z_1 z_5 \tag{3.36}$$
$$(\lambda_{27} - \lambda_{44}) z_0 z_3 - \rho_{44} z_4^2 + \rho_{27} z_2 z_7 \tag{3.37}$$
$$(\lambda_{68} - \lambda_{44}) z_0 z_3 - \rho_{44} z_4^2 + \rho_{68} z_6 z_8 \tag{3.38}$$
$$(\lambda_{18} - \lambda_{33}) z_0 z_4 - \rho_{33} z_3^2 + \rho_{18} z_1 z_8 \tag{3.39}$$
$$(\lambda_{26} - \lambda_{33}) z_0 z_4 - \rho_{33} z_3^2 + \rho_{26} z_2 z_6 \tag{3.40}$$
$$(\lambda_{57} - \lambda_{33}) z_0 z_4 - \rho_{33} z_3^2 + \rho_{57} z_5 z_7 \tag{3.41}$$
$$(\lambda_{17} - \lambda_{66}) z_0 z_5 - \rho_{66} z_6^2 + \rho_{17} z_1 z_7 \tag{3.42}$$
$$(\lambda_{23} - \lambda_{66}) z_0 z_5 - \rho_{66} z_6^2 + \rho_{23} z_2 z_3 \tag{3.43}$$
$$(\lambda_{48} - \lambda_{66}) z_0 z_5 - \rho_{66} z_6^2 + \rho_{48} z_4 z_8 \tag{3.44}$$
$$(\lambda_{14} - \lambda_{55}) z_0 z_6 - \rho_{55} z_5^2 + \rho_{14} z_1 z_4 \tag{3.45}$$
$$(\lambda_{28} - \lambda_{55}) z_0 z_6 - \rho_{55} z_5^2 + \rho_{28} z_2 z_8 \tag{3.46}$$
$$(\lambda_{37} - \lambda_{55}) z_0 z_6 - \rho_{55} z_5^2 + \rho_{37} z_3 z_7 \tag{3.47}$$
$$(\lambda_{13} - \lambda_{88}) z_0 z_7 - \rho_{88} z_8^2 + \rho_{13} z_1 z_3 \tag{3.48}$$
$$(\lambda_{25} - \lambda_{88}) z_0 z_7 - \rho_{88} z_8^2 + \rho_{25} z_2 z_5 \tag{3.49}$$
$$(\lambda_{46} - \lambda_{88}) z_0 z_7 - \rho_{88} z_8^2 + \rho_{46} z_4 z_6 \tag{3.50}$$
$$(\lambda_{16} - \lambda_{77}) z_0 z_8 - \rho_{77} z_7^2 + \rho_{16} z_1 z_6 \tag{3.51}$$
$$(\lambda_{24} - \lambda_{77}) z_0 z_8 - \rho_{77} z_7^2 + \rho_{24} z_2 z_4 \tag{3.52}$$
$$(\lambda_{35} - \lambda_{77}) z_0 z_8 - \rho_{77} z_7^2 + \rho_{35} z_3 z_5 \tag{3.53}$$

3.5.1 Calculating the Covering Curve

The 27 quadrics above describe a 3-covering of E. In Section 3.4.2, we described a method to obtain equations for the associated $\hat{\phi}$-covering of E, through which this 3-covering factors. We calculated this equation before, in Section 3.4, where we calculated the covering curve C_v in (2.15). We will now show that we obtain the same equation by eliminating the variables $z_3, \ldots z_8$ from the ideal above.

From equations (3.27), (3.31), (3.34), (3.36) and (3.37) we obtain the following.

$$\begin{aligned}&\frac{1}{\beta}(\lambda_{27}-\lambda_{15})z_0(3.27)+\frac{\rho_{12}}{\beta}z_2(3.31)-\frac{\rho_{12}}{\beta}z_1(3.34)+\frac{\rho_{34}}{\beta}z_4(3.36)-\frac{\rho_{34}}{\beta}z_4(3.37)\\&=(\lambda_{27}-\lambda_{15})z_0^3+\frac{\rho_{11}\rho_{12}}{\beta}z_1^3-\frac{\rho_{12}\rho_{22}}{\beta}z_2^3+\frac{\rho_{12}}{\beta}(\lambda_{15}-\lambda_{27}+\lambda_{47}-\lambda_{22}+\lambda_{11}-\lambda_{45})z_0z_1z_2\end{aligned}$$

Similarly, we obtain the following two terms

$$\begin{aligned}&\frac{1}{\sigma^2(\beta)}(\lambda_{23}-\lambda_{17})z_0(3.28)+\frac{\rho_{12}}{\sigma^2(\beta)}z_2(3.30)-\frac{\rho_{12}}{\sigma^2(\beta)}z_1(3.35)+\frac{\rho_{56}}{\sigma^2(\beta)}z_6(3.42)-\frac{\rho_{56}}{\sigma^2(\beta)}z_6(3.43)\\&=(\lambda_{23}-\lambda_{17})z_0^3+\frac{\rho_{11}\rho_{12}}{\sigma^2(\beta)}z_1^3-\frac{\rho_{12}\rho_{22}}{\sigma^2(\beta)}z_2^3+\frac{\rho_{12}}{\sigma^2(\beta)}(\lambda_{17}-\lambda_{23}+\lambda_{36}-\lambda_{22}+\lambda_{11}-\lambda_{67})z_0z_1z_2\end{aligned}$$

and

$$\begin{aligned}&\frac{1}{\sigma(\beta)}(\lambda_{25}-\lambda_{13})z_0(3.29)+\frac{\rho_{12}}{\sigma(\beta)}z_2(3.32)-\frac{\rho_{12}}{\sigma(\beta)}z_1(3.33)+\frac{\rho_{78}}{\sigma(\beta)}z_8(3.48)-\frac{\rho_{78}}{\sigma(\beta)}z_8(3.49)\\&=(\lambda_{25}-\lambda_{13})z_0^3+\frac{\rho_{11}\rho_{12}}{\sigma(\beta)}z_1^3-\frac{\rho_{12}\rho_{22}}{\sigma(\beta)}z_2^3+\frac{\rho_{12}}{\sigma(\beta)}(\lambda_{13}-\lambda_{25}+\lambda_{58}-\lambda_{22}+\lambda_{11}-\lambda_{38})z_0z_1z_2.\end{aligned}$$

Adding all three together gives us the following:

$$\begin{aligned}&(\lambda_{27}-\lambda_{15}+\lambda_{23}-\lambda_{17}+\lambda_{25}-\lambda_{13})z_0^3+\rho_{11}\rho_{12}\left(\frac{1}{\beta}+\frac{1}{\sigma(\beta)}+\frac{1}{\sigma^2(\beta)}\right)z_1^3\\&-\rho_{12}\rho_{22}\left(\frac{1}{\beta}+\frac{1}{\sigma(\beta)}+\frac{1}{\sigma^2(\beta)}\right)z_2^3+\rho_{12}\left(\frac{1}{\beta}(\lambda_{15}-\lambda_{27}+\lambda_{47}-\lambda_{22}+\lambda_{11}-\lambda_{45})\right.\\&\left.+\frac{1}{\sigma^2(\beta)}(\lambda_{17}-\lambda_{23}+\lambda_{36}-\lambda_{22}+\lambda_{11}-\lambda_{67})+\frac{1}{\sigma(\beta)}(\lambda_{13}-\lambda_{25}+\lambda_{58}-\lambda_{22}+\lambda_{11}-\lambda_{38})\right)z_0z_1z_2=0\end{aligned}\tag{3.54}$$

From the fact that β is a root of $\psi(x)=3x^3+4\varepsilon^2\Delta x^2+12\varepsilon\eta\Delta x+12\eta^2\Delta$ we get that

$$\begin{aligned}\beta\sigma(\beta)\sigma^2(\beta)&=-4\eta^2\Delta\\\beta\sigma(\beta)+\beta\sigma^2(\beta)+\sigma(\beta)\sigma^2(\beta)&=4\varepsilon\eta\Delta\\\beta+\sigma(\beta)+\sigma^2(\beta)&=-\frac{4}{3}\varepsilon^2\Delta.\end{aligned}$$

Using these facts, we find that equation (3.54) simplifies to

$$-2\varepsilon\sqrt{\Delta}z_0^3-\frac{\varepsilon}{\eta}\gamma_1^3z_1^3+\frac{\varepsilon}{\eta}\gamma_2^3z_2^3-2\frac{\varepsilon^2}{\eta}\sqrt{\Delta}\gamma_1\gamma_2z_0z_1z_2=0\tag{3.55}$$

which we multiply by $-\frac{\eta}{\varepsilon\gamma_1\gamma_2}$ and send $z_2\mapsto -z_2$ to obtain

$$2\varepsilon\sqrt{\Delta}z_0z_1z_2+\frac{2\eta\sqrt{\Delta}}{\gamma_1\gamma_2}z_0^3+\frac{\gamma_1^2}{\gamma_2}z_1^3+\frac{\gamma_2^2}{\gamma_1}z_2^3=0.$$

In the case that $\Delta=1$, we find that $\gamma_2=\frac{1}{\gamma_1}$, and therefore we obtain the equation we found in (2.13). In the case that $\Delta\neq 1$, we can let $\alpha_1=v^2\tau(v)$ for some $v=v_1+v_2\sqrt{\Delta}$, giving us $\gamma_1\gamma_2=v\tau(v)$ and

$$C'_v: 2\varepsilon\sqrt{\Delta}z_0z_1z_2+\frac{2\eta\sqrt{\Delta}}{v\tau(v)}z_0^3+vz_1^3-\tau(v)z_2^3=0$$

which is the same as the equation we found in (2.14).

3.5.2 Calculating the Pushout Form

The pushout form is calculated as described in Section 3.4. First we create a cubic of the proper divisor:

$$(z_3+z_5+z_7)^3 = z_3^3+z_5^3+z_7^3+3z_3^2z_5+3z_3z_5^2+3z_5^2z_7+3z_5z_7^2+3z_3^2z_7+3z_3z_7^2+6z_3z_5z_7 \tag{3.56}$$

We now proceed to substitute in the appropriate terms. For example, to get rid of the $z_3^2z_5$ term, we use the following obtained by multiplying equation (3.39) by z_5.

$$\rho_{33}z_3^2z_5 = \rho_{18}z_1z_5z_8 + (\lambda_{18}-\lambda_{33})z_0z_4z_5$$

We now substitute in $z_5z_8 = \frac{\rho_{22}}{\rho_{58}}z_2^2 + \frac{(\lambda_{22}-\lambda_{58})}{\rho_{58}}z_0z_1$ from equation (3.32) and $z_4z_5 = \frac{\rho_{11}}{\rho_{45}}z_1^2 + \frac{(\lambda_{11}-\lambda_{45})}{\rho_{45}}z_0z_2$ from equation (3.34) to obtain the following.

$$z_3^2z_5 = \left(\frac{(\lambda_{18}-\lambda_{33})\rho_{11}}{\rho_{45}\rho_{33}} + \frac{(\lambda_{22}-\lambda_{58})\rho_{18}}{\rho_{58}\rho_{33}}\right)z_0z_1^2 + \frac{(\lambda_{18}-\lambda_{33})(\lambda_{11}-\lambda_{45})}{\rho_{45}\rho_{33}}z_0^2z_2 + \frac{\rho_{18}\rho_{22}}{\rho_{58}\rho_{33}}z_1z_2^2$$

We obtain similarly for the other 'mixed' terms

$$\begin{aligned}
z_3\cdot(3.46):\ z_3z_5^2 &= \left(\frac{(\lambda_{28}-\lambda_{55})\rho_{22}}{\rho_{36}\rho_{55}} + \frac{(\lambda_{11}-\lambda_{38})\rho_{28}}{\rho_{38}\rho_{55}}\right)z_0z_2^2 + \frac{(\lambda_{28}-\lambda_{55})(\lambda_{22}-\lambda_{36})}{\rho_{36}\rho_{55}}z_0^2z_1 + \frac{\rho_{28}\rho_{11}}{\rho_{38}\rho_{55}}z_1^2z_2\\
z_7\cdot(3.45):\ z_5^2z_7 &= \left(\frac{(\lambda_{14}-\lambda_{55})\rho_{11}}{\rho_{67}\rho_{55}} + \frac{(\lambda_{22}-\lambda_{47})\rho_{14}}{\rho_{47}\rho_{55}}\right)z_0z_1^2 + \frac{(\lambda_{14}-\lambda_{55})(\lambda_{11}-\lambda_{67})}{\rho_{67}\rho_{55}}z_0^2z_2 + \frac{\rho_{14}\rho_{22}}{\rho_{47}\rho_{55}}z_1z_2^2\\
z_5\cdot(3.52):\ z_5z_7^2 &= \left(\frac{(\lambda_{24}-\lambda_{77})\rho_{22}}{\rho_{58}\rho_{77}} + \frac{(\lambda_{11}-\lambda_{45})\rho_{24}}{\rho_{45}\rho_{77}}\right)z_0z_2^2 + \frac{(\lambda_{24}-\lambda_{77})(\lambda_{22}-\lambda_{58})}{\rho_{58}\rho_{77}}z_0^2z_1 + \frac{\rho_{24}\rho_{11}}{\rho_{45}\rho_{77}}z_1^2z_2\\
z_7\cdot(3.40):\ z_3^2z_7 &= \left(\frac{(\lambda_{26}-\lambda_{33})\rho_{22}}{\rho_{47}\rho_{33}} + \frac{(\lambda_{11}-\lambda_{67})\rho_{26}}{\rho_{67}\rho_{33}}\right)z_0z_2^2 + \frac{(\lambda_{26}-\lambda_{33})(\lambda_{22}-\lambda_{47})}{\rho_{47}\rho_{33}}z_0^2z_1 + \frac{\rho_{26}\rho_{11}}{\rho_{67}\rho_{33}}z_1^2z_2\\
z_3\cdot(3.51):\ z_3z_7^2 &= \left(\frac{(\lambda_{16}-\lambda_{77})\rho_{11}}{\rho_{38}\rho_{77}} + \frac{(\lambda_{22}-\lambda_{36})\rho_{16}}{\rho_{36}\rho_{77}}\right)z_0z_1^2 + \frac{(\lambda_{16}-\lambda_{77})(\lambda_{11}-\lambda_{38})}{\rho_{38}\rho_{77}}z_0^2z_2 + \frac{\rho_{16}\rho_{22}}{\rho_{36}\rho_{77}}z_1z_2^2
\end{aligned} \tag{3.57}$$

We now tackle the final $z_3z_5z_7$ term. We want to express it as the trace of some expression, therefore we will need three different ways of writing it. From equation (3.41) we obtain

$$\rho_{57}z_3z_5z_7 = \rho_{33}z_3^3 + (\lambda_{33}-\lambda_{57})z_0z_3z_4.$$

Substituting in from equation (3.27) gives us

$$z_3z_5z_7 = \frac{\rho_{33}}{\rho_{57}}z_3^3 + \frac{(\lambda_{33}-\lambda_{57})\rho_{12}}{\rho_{34}\rho_{57}}z_0z_1z_2 + \frac{(\lambda_{57}-\lambda_{33})\beta}{\rho_{34}\rho_{57}}z_0^3. \tag{3.58}$$

Similarly, starting with equations (3.47) and (3.53) respectively we get

$$z_3z_5z_7 = \frac{\rho_{55}}{\rho_{37}}z_5^3 + \frac{(\lambda_{55}-\lambda_{37})\rho_{12}}{\rho_{56}\rho_{37}}z_0z_1z_2 + \frac{(\lambda_{37}-\lambda_{55})\sigma^2(\beta)}{\rho_{56}\rho_{37}}z_0^3 \tag{3.59}$$

$$z_3z_5z_7 = \frac{\rho_{77}}{\rho_{35}}z_7^3 + \frac{(\lambda_{77}-\lambda_{35})\rho_{12}}{\rho_{78}\rho_{35}}z_0z_1z_2 + \frac{(\lambda_{35}-\lambda_{77})\sigma(\beta)}{\rho_{78}\rho_{35}}z_0^3. \tag{3.60}$$

Combining the three equations (3.58), (3.59) and (3.60) equally gives us

$$\begin{aligned}
6z_3z_5z_7 = {} & \frac{2\rho_{33}}{\rho_{57}}z_3^3 + \frac{2\rho_{55}}{\rho_{37}}z_5^3 + \frac{2\rho_{77}}{\rho_{35}}z_7^3 + 2\rho_{12}\left(\frac{(\lambda_{33}-\lambda_{57})}{\rho_{34}\rho_{57}} + \frac{(\lambda_{55}-\lambda_{37})}{\rho_{56}\rho_{37}} + \frac{(\lambda_{77}-\lambda_{35})}{\rho_{78}\rho_{35}}\right)z_0z_1z_2\\
& + 2\left(\frac{(\lambda_{57}-\lambda_{33})\beta}{\rho_{34}\rho_{57}} + \frac{(\lambda_{37}-\lambda_{55})\sigma^2(\beta)}{\rho_{56}\rho_{37}} + \frac{(\lambda_{35}-\lambda_{77})\sigma(\beta)}{\rho_{78}\rho_{35}}\right)z_0^3
\end{aligned} \tag{3.61}$$

Now all that is left are the cubed terms z_3^3, z_5^3 and z_7^3. To substitute for these, we need Proposition 3.4.8. Let l_i be the tangent line at $T_i \in E[3]$. Then $\mathrm{div}(l_i) = 3(T_i) - 3(\mathscr{O})$, and therefore we have $y - \lambda_{ii}x - c_i = \alpha_i z_i^3$ for all $i \in \{1,\ldots,8\}$. In particular, we have

$$\begin{aligned} y - \lambda_{33}x - c_3 &= \alpha_3 z_3^3 \\ y - \lambda_{55}x - c_5 &= \alpha_5 z_5^3 \\ y - \lambda_{77}x - c_7 &= \alpha_7 z_7^3 \end{aligned} \tag{3.62}$$

and

$$y - \lambda_{11}x - c_1 = y - \sqrt{\Delta}(\varepsilon x + \eta) = \alpha_1 z_1^3 \tag{3.63}$$

$$y - \lambda_{22}x - c_2 = y + \sqrt{\Delta}(\varepsilon x + \eta) = \alpha_2 z_2^3. \tag{3.64}$$

Multiplying(3.63) and (3.64) together gives

$$\left(y - \sqrt{\Delta}(\varepsilon x + \eta)\right)\left(y + \sqrt{\Delta}(\varepsilon x + \eta)\right) = x^3 = \alpha_1\alpha_2 z_1^3 z_2^3$$

or, after homogenizing

$$x = \rho_{12} z_0 z_1 z_2. \tag{3.65}$$

By adding the equations we get for y

$$y = \frac{1}{2}(\alpha_1 z_1^3 + \alpha_2 z_2^3). \tag{3.66}$$

Substituting (3.65) and (3.66) into (3.62) and homogenizing, we get the following

$$\begin{aligned} z_3^3 &= \frac{\alpha_1}{2\alpha_3} z_1^3 + \frac{\alpha_2}{2\alpha_3} z_2^3 - \frac{\lambda_{33}\rho_{12}}{\alpha_3} z_0 z_1 z_2 - \frac{c_3}{a_3} z_0^3 \\ z_5^3 &= \frac{\alpha_1}{2\alpha_5} z_1^3 + \frac{\alpha_2}{2\alpha_5} z_2^3 - \frac{\lambda_{55}\rho_{12}}{\alpha_5} z_0 z_1 z_2 - \frac{c_5}{a_5} z_0^3 \\ z_7^3 &= \frac{\alpha_1}{2\alpha_7} z_1^3 + \frac{\alpha_2}{2\alpha_7} z_2^3 - \frac{\lambda_{77}\rho_{12}}{\alpha_7} z_0 z_1 z_2 - \frac{c_7}{a_7} z_0^3 \end{aligned} \tag{3.67}$$

These cubics also lie in the ideal generated by the quadrics in the previous section. By substituting into (3.56) the results from (3.57), (3.61) and (3.67) we get the following equation for the pushout form.

$$
\begin{aligned}
&z_0^3\left\{\frac{2\beta(\lambda_{57}-\lambda_{33})}{\rho_{34}\rho_{57}}+\frac{2\sigma^2(\beta)(\lambda_{37}-\lambda_{55})}{\rho_{56}\rho_{37}}+\frac{2\sigma(\beta)(\lambda_{35}-\lambda_{77})}{\rho_{78}\rho_{35}}-\frac{c_3(\rho_{57}+2\rho_{33})}{\alpha_3\rho_{57}}\right.\\
&\quad\left.-\frac{c_5(\rho_{37}+2\rho_{55})}{\alpha_5\rho_{37}}-\frac{c_7(\rho_{35}+2\rho_{77})}{\alpha_7\rho_{35}}\right\}\\
&+z_1^3\left\{\frac{\alpha_1(\rho_{57}+2\rho_{33})}{2\alpha_3\rho_{57}}+\frac{\alpha_1(\rho_{37}+2\rho_{55})}{2\alpha_5\rho_{37}}+\frac{\alpha_1(\rho_{35}+2\rho_{77})}{2\alpha_7\rho_{35}}\right\}\\
&+z_2^3\left\{\frac{\alpha_2(\rho_{57}+2\rho_{33})}{2\alpha_3\rho_{57}}+\frac{\alpha_2(\rho_{37}+2\rho_{55})}{2\alpha_5\rho_{37}}+\frac{\alpha_2(\rho_{35}+2\rho_{77})}{2\alpha_7\rho_{35}}\right\}\\
&+z_0^2z_1\left\{\frac{3(\lambda_{26}-\lambda_{33})(\lambda_{22}-\lambda_{47})}{\rho_{47}\rho_{33}}+\frac{3(\lambda_{28}-\lambda_{55})(\lambda_{22}-\lambda_{36})}{\rho_{36}\rho_{55}}+\frac{3(\lambda_{24}-\lambda_{77})(\lambda_{22}-\lambda_{58})}{\rho_{58}\rho_{77}}\right\}\\
&+z_0z_1^2\left\{\frac{3(\lambda_{18}-\lambda_{33})\rho_{11}}{\rho_{45}\rho_{33}}+\frac{3(\lambda_{14}-\lambda_{55})\rho_{11}}{\rho_{67}\rho_{55}}+\frac{3(\lambda_{16}-\lambda_{77})\rho_{11}}{\rho_{38}\rho_{77}}+\frac{3(\lambda_{22}-\lambda_{58})\rho_{18}}{\rho_{58}\rho_{33}}\right.\\
&\quad\left.+\frac{3(\lambda_{22}-\lambda_{47})\rho_{14}}{\rho_{47}\rho_{55}}+\frac{3(\lambda_{22}-\lambda_{36})\rho_{16}}{\rho_{36}\rho_{77}}\right\}\\
&+z_0^2z_2\left\{\frac{3(\lambda_{18}-\lambda_{33})(\lambda_{11}-\lambda_{45})}{\rho_{45}\rho_{33}}+\frac{3(\lambda_{14}-\lambda_{55})(\lambda_{11}-\lambda_{67})}{\rho_{67}\rho_{55}}+\frac{3(\lambda_{16}-\lambda_{77})(\lambda_{11}-\lambda_{38})}{\rho_{38}\rho_{77}}\right\}\\
&+z_0z_2^2\{\frac{3(\lambda_{28}-\lambda_{55})\rho_{22}}{\rho_{36}\rho_{55}}+\frac{3(\lambda_{26}-\lambda_{33})\rho_{22}}{\rho_{47}\rho_{33}}+\frac{3(\lambda_{24}-\lambda_{77})\rho_{22}}{\rho_{58}\rho_{77}}+\frac{3(\lambda_{11}-\lambda_{67})\rho_{26}}{\rho_{67}\rho_{33}}\\
&\quad+\frac{3(\lambda_{11}-\lambda_{38})\rho_{28}}{\rho_{38}\rho_{55}}+\frac{3(\lambda_{11}-\lambda_{45})\rho_{24}}{\rho_{45}\rho_{77}}\}\\
&+z_1^2z_2\left\{3\frac{\rho_{26}\rho_{11}}{\rho_{67}\rho_{33}}+3\frac{\rho_{28}\rho_{11}}{\rho_{38}\rho_{55}}+3\frac{\rho_{24}\rho_{11}}{\rho_{45}\rho_{77}}\right\}\\
&+z_1z_2^2\left\{3\frac{\rho_{18}\rho_{22}}{\rho_{58}\rho_{33}}+3\frac{\rho_{14}\rho_{22}}{\rho_{47}\rho_{55}}+3\frac{\rho_{16}\rho_{22}}{\rho_{36}\rho_{77}}\right\}\\
&+z_0z_1z_2\left\{-\frac{\rho_{12}\lambda_{33}(\rho_{57}+2\rho_{33})}{\alpha_3\rho_{57}}-\frac{\rho_{12}\lambda_{55}(\rho_{37}+2\rho_{55})}{\alpha_5\rho_{37}}-\frac{\rho_{12}\lambda_{77}(\rho_{35}+2\rho_{77})}{\alpha_7\rho_{35}}\right\}
\end{aligned}
\tag{3.68}
$$

This is a rather nasty formula, and we would like to simplify it if possible. We saw in Section 3.4.2 that one way to do so would be to consider the form $(\chi z_3+\sigma^2(\chi)z_5+\sigma(\chi)z_7)^3$ for some χ instead of (3.56). We might also rescale (3.68) and add multiples of the covering curve in whose function field this pushout form lies, computed in Section 3.5.1. We found no way of using either of these procedures that simplified this formula. We might also use relations between the λ's such as that in the following lemma.

Lemma 3.5.1 ([CFO+09, Lemma 4.2]). *Let $T_1,T_2,T_3\in E[3]\setminus\{\mathscr{O}\}$ with $T_1+T_2+T_3=\mathscr{O}$. Then*

$$\lambda(T_1,T_2)=\frac{1}{3}\sum_{i=1}^{3}\lambda(T_i,T_i).$$

Using this lemma, we would find $\lambda_{23}=\lambda_{26}=\lambda_{36}=\frac{1}{3}(\lambda_{22}+\lambda_{33}+\lambda_{66})$. This however does not seem to give anything much simpler either, simply yielding a formula using different λ's, but no simpler. The final method is to use ρ relations. In the following sections, we make the ρ's explicit and eliminate them from the formula, sacrificing generality for a little more simplicity.

3.5.3 μ_3-nonsplit

In this case, E is of the form (3.26) with $\Delta = -3$. Consider $u \in S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$. Let $K = \mathbb{Q}$, $L_1 = \mathbb{Q}(\zeta_3)$, $L_2 = \mathbb{Q}(\beta)$ and $M = \mathbb{Q}(\zeta_3, \beta)$ where β is a root of $x^3 - 4\varepsilon^2 x^2 - 12\varepsilon\eta x - 12\eta^2$. Let G be the subgroup of G_K through which the action of G_K on $E[3]$ factors. We have $E[3] = \langle S, T \rangle$ where S generates the kernel of ϕ, and thus

$$S = (0, \eta\sqrt{-3}) \qquad\qquad T = (\beta, \varepsilon\beta + 3\eta)$$

and $\tau, \sigma \in G$ such that

$$\begin{aligned} \tau(S) &= -S & \tau(T) &= T \\ \sigma(S) &= S & \sigma(T) &= S + T. \end{aligned}$$

From (3.55), we find that the covering curve is given by

$$C_u : 2\eta\sqrt{\Delta}z_0^3 + uz_1^3 - \tau(u)z_2^3 + 2\varepsilon\sqrt{\Delta}\rho_{12}z_0z_1z_2 = 0. \tag{3.69}$$

Let $C \in \mathbb{Q}$ be such that $N_{L_1/\mathbb{Q}}(u) = C^3$ and let ξ be such that $N_{M/L_1}(\xi) = u$. Then from Lemma 2.5.9 we find $d = \frac{\tau\sigma(\xi)\sigma(\xi)}{\sigma^2(\xi)\sigma\tau(\xi)}$ such that

$$\begin{aligned} \alpha_1 &= \alpha(S) = u & \alpha_5 &= \alpha(-S+T) = \sigma^2(d) \\ \alpha_2 &= \alpha(-S) = \tau(u) & \alpha_6 &= \alpha(S-T) = \sigma^2(d)^2 \\ \alpha_3 &= \alpha(T) = d & \alpha_7 &= \alpha(S+T) = \sigma(d) \\ \alpha_4 &= \alpha(-T) = d^2 & \alpha_8 &= \alpha(-S-T) = \sigma(d)^2 \end{aligned}$$

We now explicitly find ρ, as explained in Section 3.4.1. This means dealing with cube roots of unity. At the end of Section 3.4.1, we saw that we have $\#(\partial\Gamma)$ choices for ρ, which in this case is 3. There are 21 orbits for the action of G_K on $E[3] \times E[3]$, with representatives listed in the following table. Recall that there exists $\gamma \in \overline{R}^\times$ with $\alpha = \gamma^3$ and $\rho = \partial\gamma$, and write γ_P for $\gamma(P)$. The column in the table labelled 'in γ' expresses the element $\rho(T_1, T_2)$ as a product of the γ_P. Notice that we have $\gamma_{-T} = \gamma_T^2$. We use that ρ is symmetric and $\rho(\mathcal{O}, T_i) = 1$ for all $T_i \in E[3]$. There are three choices still to make, namely

1. $y = \gamma_S\gamma_{-S}$, a cube root of $N_{L_1/K}(\alpha_1) = C^3$.

2. $w = \gamma_T\gamma_{S+T}\gamma_{-S+T}$, a cube root of $N_{L_2/K}(d) = 1$.

3. $t = \frac{\gamma_{S+T}}{\gamma_S\gamma_T}$, a cube root of $\frac{\sigma(d)}{ud}$.

#	(T_1,T_2)	T_1+T_2	in γ	ρ	#	(T_1,T_2)	T_1+T_2	in γ	ρ
1	$(\mathscr{O},\mathscr{O})$	$\mathscr{O}$	$\gamma_{\mathscr{O}}$	1	12	$(T,-T)$	$\mathscr{O}$	$\gamma_T\gamma_{-T}$	d
2	$(S,\mathscr{O})$	S	$\gamma_{\mathscr{O}}$	1	13	$(-T,T)$	$\mathscr{O}$	$\gamma_{-T}\gamma_T$	d
3	$(T,\mathscr{O})$	T	$\gamma_{\mathscr{O}}$	1	14	$(S+T,-T)$	S	$\frac{\gamma_{S+T}\gamma_{-T}\gamma_T}{\gamma_S\gamma_T}$	dt
4	$(-T,\mathscr{O})$	$-T$	$\gamma_{\mathscr{O}}$	1	15	$(-T,S+T)$	S	$\frac{\gamma_{-T}\gamma_{S+T}\gamma_T}{\gamma_S\gamma_T}$	dt
5	$(\mathscr{O},S)$	S	$\gamma_{\mathscr{O}}$	1	16	$(S-T,-S-T)$	T	$\frac{\gamma_{S-T}\gamma_{-S-T}\gamma_{-T}}{\gamma_T\gamma_{-T}}$	$\frac{w^2}{d}$
6	$(\mathscr{O},T)$	T	$\gamma_{\mathscr{O}}$	1	17	$(S+T,-S+T)$	$-T$	$\frac{\gamma_{S+T}\gamma_{-S+T}\gamma_T}{\gamma_{-T}\gamma_T}$	$\frac{w}{d}$
7	$(\mathscr{O},-T)$	$-T$	$\gamma_{\mathscr{O}}$	1	18	$(-S,S+T)$	T	$\frac{\gamma_{-S}\gamma_{S+T}\gamma_S}{\gamma_T\gamma_S}$	yt
8	(S,S)	$-S$	$\frac{\gamma_S^2}{\gamma_{-S}}$	$\frac{u}{y}$	19	$(S,-S-T)$	$-T$	$\frac{\gamma_{-S-T}\gamma_S^3}{\gamma_{-T}\gamma_S^2}$	ut^2
9	$(-T,-T)$	T	$\frac{\gamma_{-T}^2}{\gamma_T}$	d	20	$(S+T,-S)$	T	$\frac{\gamma_{S+T}\gamma_{-S}\gamma_S}{\gamma_T\gamma_S}$	yt
10	(T,T)	$-T$	$\frac{\gamma_T^2}{\gamma_{-T}}$	1	21	$(-S-T,S)$	$-T$	$\frac{\gamma_{-S-T}\gamma_S^3}{\gamma_{-T}\gamma_S^2}$	ut^2
11	$(S,-S)$	$\mathscr{O}$	$\gamma_S\gamma_{-S}$	y					

We now use Lemma 3.4.6 to reduce the number of choices here. Because of the symmetry condition, we have $\rho(S,-S)=\rho(-S,S)$, thus we must choose y such that $y=\tau(y)$, giving us $y=C$. The symmetry condition also gives us $\rho(S+T,-S+T)=\rho(-S+T,S+T)$ thus we must choose w such that $\frac{w}{d}=\frac{\tau(v)}{\tau(d)}$. Of course, d is invariant under τ, so we have $w=\tau(w)$, and so $w=1$. This leaves three choices for t, all of which are permitted. We have

$$\begin{aligned} t^3 &= \frac{\sigma(d)}{ud} = \frac{\tau(\xi)\sigma^2(\xi)\sigma\tau(\xi)}{u\xi\,\tau\sigma(\xi)^2\sigma^2(\xi)} \\ &= \frac{C^3\sigma^2(\xi)^3}{u^3\tau\sigma(\xi)^3} \end{aligned}$$

and so, summarizing, we make the following choices. Note that taking $t=\zeta_3^i t$ for some i is equally valid.

$$y=C \qquad\qquad w=1 \qquad\qquad t=\frac{C\sigma^2(\xi)}{u\tau\sigma(\xi)}$$

Let us now simplify the coefficient for the z_0^3 term of (3.68). We have

$$\begin{aligned} \rho_{34}\rho_{57}=\rho_{56}\rho_{37}=\rho_{78}\rho_{35}=\gamma_3\gamma_5\gamma_7 \\ \frac{\rho_{33}}{\alpha_3\rho_{57}}=\frac{\rho_{55}}{\alpha_5\rho_{37}}=\frac{\rho_{77}}{\alpha_7\rho_{35}}=\gamma_3\gamma_5\gamma_7 \end{aligned}$$

and

$$\rho_{34}\rho_{57}=\rho(T,-T)\rho(-S-T,S+T)=\frac{d\tau(w)}{\tau(d)}=1.$$

Therefore the coefficient of z_0 becomes

$$\Xi = Tr_{M/L_1}\left(2\beta(\lambda_{57}-\lambda_{33})-c_3\left(2+\frac{1}{d}\right)\right). \tag{3.70}$$

Similarly, we obtain

$$\begin{aligned}
\Pi &= Tr_{L_2/\mathbb{Q}}\left(1+\frac{1}{2d}\right)\\
\Sigma &= \frac{3u}{C}Tr_{M/L_1}\left(\frac{\tau(\xi)}{\xi}(\lambda_{28}-\lambda_{55})(\lambda_{22}-\lambda_{36})\right)\\
\Upsilon &= 3C\,Tr_{M/L_1}\left(\frac{\xi}{\tau(\xi)}(\lambda_{16}-\lambda_{77}+\lambda_{22}-\lambda_{36})\right)\\
\Phi &= 3uTr_{M/L_1}\left(\frac{\tau(\xi)}{\xi}\right)\\
\Psi &= -C\,Tr_{M/L_1}\left(\lambda_{33}\left(2+\frac{1}{d}\right)\right)
\end{aligned} \tag{3.71}$$

where the pushout form is given by

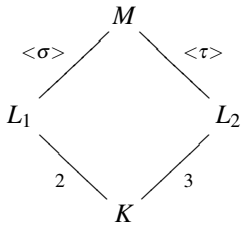
$$\Xi z_0^3+\Pi\left(uz_1^3+\tau(u)z_2^3\right)+\Sigma z_0^2z_1+\tau(\Sigma)z_0^2z_2+\Upsilon z_0z_1^2+\tau(\Upsilon)z_0z_2^2+\Phi z_1^2z_2+\tau(\Phi)z_1z_2^2+\Psi z_0z_1z_2. \tag{3.72}$$

We can substitute

$$\begin{aligned}
z_0 &= Z\\
z_1 &= X-\sqrt{-3}Y\\
z_2 &= X+\sqrt{-3}Y
\end{aligned}$$

to give us a covering curve and pushout form defined over $\mathbb{Q}$. We can now give an example of computing pushout forms.

Example 3.5.2. Let $E: y^2=x^3-3(4x+28)^2$, with Cremona reference 24003d1. This curve admits a 3-isogeny ϕ and the isogenous curve $\hat{E}$ is given by $\hat{E}: y^2=x^3+(12x+508)^2$. Thus $E[\phi]\cong\mu_3$ and $\hat{E}[\hat{\phi}]\cong\mathbb{Z}/3\mathbb{Z}$ as Galois modules and we are in the μ_3-nonsplit case as defined in Section 2.5. Let $L_1=\mathbb{Q}(\zeta_3)$, $L_2=\mathbb{Q}(\beta)$ and $M=\mathbb{Q}(\zeta_3,\beta)$ where $\beta^3=127$. Let $G_{M/\mathbb{Q}}$ be generated by $\langle\tau,\sigma\rangle$ such that we have the following diagram.



We then have $E[3]=\langle S,T\rangle$, where $\langle S\rangle$ is the kernel of the isogeny ϕ and

$$\begin{aligned}
S &= (0,56\zeta_3+28)\\
T &= \left(\frac{4}{3}\beta^2+\frac{16}{3}\beta+\frac{64}{3},\frac{16}{3}\beta^2+\frac{64}{3}\beta+\frac{508}{3}\right).
\end{aligned}$$

By doing a descent by 3-isogeny we obtain

$$S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})=\langle\zeta_3,-14\zeta_3+7\rangle.$$

From Section 2.5.1 we know that these generators are both norms for the extension M/L_1, so for $u\in S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ there exists $\xi\in M$ such that $\xi\sigma(\xi)\sigma^2(\xi)=a$. The table below contains a ξ for each generator of $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$, as well as the element d that we need to construct pushout forms.

u	ξ	d
ζ_3	$\frac{1}{9}(-547\zeta_3-92)\beta^2+\frac{1}{9}(659\zeta_3-2282)\beta+\frac{1}{9}(10508\zeta_3+13795)$	$-\frac{2}{9}\beta^2-\frac{17}{9}\beta+\frac{136}{9}$
$-14\zeta_3+7$	$\frac{1}{3}(-812\zeta_3-262)\beta^2+\frac{1}{3}(-4082\zeta_3-1318)\beta+\frac{1}{3}(-20513\zeta_3-6622)$	$\frac{886}{7}\beta^2+\frac{1710}{7}\beta-\frac{30981}{7}$

We have the following covering curves, obtained from (3.69).

$S^{(\hat{\phi})}(\hat{E}/K)$	covering curve
ζ_3	$x^3-3x^2y+8x^2z-9xy^2+3y^3+24y^2z+56z^3=0$
$-14\zeta_3+7$	$-14x^3+84x^2y+56x^2z+126xy^2-84y^3+168y^2z+56z^3=0$

We have the following pushout forms, obtained from (3.72).

$S^{(\hat{\phi})}(\hat{E}/K)$	pushout forms
ζ_3	$-3623x^3-22185x^2y-74736x^2z+17811xy^2-27324xyz+22716xz^2+19485y^3$ $-175500y^2z+170100yz^2+3485696z^3$
$-14\zeta_3+7$	$657932511x^3+2961301698x^2y-4624071108x^2z-5919560811xy^2+5015304xyz$ $+6662208xz^2-2956132422y^3-13859226756y^2z-10232208yz^2+34704241748z^3$

The divisor on each pushout form f_1 is given by $\operatorname{div}\left(\frac{f_1}{x^3}\right)=3\cdot H_f-3\cdot H$, where the following table contains H_f for each generator.

$S^{(\hat{\phi})}(\hat{E}/K)$	H_f
ζ_3	$\left(\frac{1}{181}(111\alpha^2-42\alpha-1568):\alpha:1\right)$
$-14\zeta_3+7$	$\left(\frac{1}{711671}(-1294842\gamma^2+337764\gamma+2523106):\gamma:1\right)$

where we have

$$111\alpha^3-36\alpha^2-2397\alpha+62=0 \qquad 3884526\gamma^3+2043\gamma^2-11353386\gamma-1977814=0.$$

thus we see that these are indeed pushout forms.

3.5.4 $\mathbb{Z}/3\mathbb{Z}$-nonsplit

In this case, E is of the form (3.26) with $\Delta=1$. Consider $u\in S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$. Let $L_1=\mathbb{Q}(\zeta_3)$ and $M=\mathbb{Q}(\zeta_3,\beta)$ where β is a root of $x^3+\frac{4}{3}\varepsilon^2x^2+4\varepsilon\eta x+4\eta^2$. Let G be the subgroup of G_K through which the action of G_K on $E[3]$ factors. We have $E[3]=\langle S,T\rangle$ where S generates the kernel of ϕ, and thus

$$S=(0,\eta) \qquad T=\left(\beta,\frac{(\varepsilon\beta+3\eta)}{\sqrt{-3}}\right)$$

and τ,σ such that

$$\tau(S)=S \qquad \sigma(S)=S$$
$$\tau(T)=2T \qquad \sigma(T)=S+T.$$

Let ξ be such that $N_{M/L_1}(\xi) = u$. From (3.55) the covering curve is given by

$$C_u : u^2X^3 - uY^3 + 2\eta Z^3 + 2\varepsilon uXYZ = 0. \tag{3.73}$$

Then from Lemma 2.5.12 we get $d = \frac{\sigma(\xi)\sigma\tau(\xi)}{\sigma^2(\xi)\tau\sigma(\xi)}$ and let

$$\begin{aligned} \alpha_1 &= u^2 & \alpha_5 &= \tau\sigma(d) \\ \alpha_2 &= u & \alpha_6 &= \sigma^2(d) \\ \alpha_3 &= \tau(d) & \alpha_7 &= \sigma\tau(d) \\ \alpha_4 &= d & \alpha_8 &= \sigma(d) \end{aligned}$$

Once again, we make ρ explicit as explained in Section 3.4.1. By the discussion at the end of that section, the choice of ρ is unique in this case. There are 21 orbits for the action of G_K on $E[3] \times E[3]$, with representatives listed in the following table. Recall that there exists $\gamma \in \overline{R}^\times$ with $\alpha = \gamma^3$ and $\rho = \partial\gamma$, and write γ_P for $\gamma(P)$. The column labelled 'in γ' expresses the element $\rho(T_1, T_2)$ as a product of the γ_P. Notice that we have $\gamma_{-S}^2 = \gamma_S$. There are three choices of cube roots to make in the table, namely the following.

1. $v = \frac{\gamma_{S+T}}{\gamma_S\gamma_T}$, a cube root of $\frac{\sigma(d)}{\alpha_1 d}$.
2. $w = \gamma_T\gamma_{-T}$, a cube root of $N_{M/L_2}(d) = 1$.
3. $y = \gamma_T\gamma_{S+T}\gamma_{-S+T}$, a cube root of $N_{M/L_1}(d) = 1$.

#	(T_1,T_2)	T_1+T_2	in γ	ρ	#	(T_1,T_2)	T_1+T_2	in γ	ρ
1	$(\mathscr{O},\mathscr{O})$	$\mathscr{O}$	$\gamma_{\mathscr{O}}$	1	12	(T,S)	$S+T$	$\frac{\gamma_S\gamma_T}{\gamma_{S+T}}$	$\frac{1}{v}$
2	$(S,\mathscr{O})$	S	$\gamma_{\mathscr{O}}$	1	13	(S,T)	$S+T$	$\frac{\gamma_S\gamma_T}{\gamma_{S+T}}$	$\frac{1}{v}$
3	$(-S,\mathscr{O})$	$-S$	$\gamma_{\mathscr{O}}$	1	14	$(S+T,-S)$	T	$\frac{\gamma_{S+T}\gamma_{-S}\gamma_S}{\gamma_T\gamma_S}$	uv
4	$(T,\mathscr{O})$	T	$\gamma_{\mathscr{O}}$	1	15	$(-S,S+T)$	T	$\frac{\gamma_S\gamma_{-S}\gamma_{S+T}}{\gamma_S\gamma_T}$	uv
5	$(\mathscr{O},S)$	S	$\gamma_{\mathscr{O}}$	1	16	(T,T)	$-T$	$\frac{\gamma_T^3}{\gamma_T\gamma_{-T}}$	$\frac{\tau(d)}{w}$
6	$(\mathscr{O},-S)$	$-S$	$\gamma_{\mathscr{O}}$	1	17	$(-S+T,S+T)$	$-T$	$\frac{\gamma_T\gamma_{-S+T}\gamma_{S+T}}{\gamma_T\gamma_{-T}}$	$\frac{y}{w}$
7	$(\mathscr{O},T)$	T	$\gamma_{\mathscr{O}}$	1	18	$(S+T,-S+T)$	$-T$	$\frac{\gamma_{-S+T}\gamma_{S+T}\gamma_T}{\gamma_T\gamma_{-T}}$	$\frac{y}{w}$
8	(S,S)	$-S$	$\frac{\gamma_S^3}{\gamma_S\gamma_{-S}}$	u	19	$(-T,T)$	$\mathscr{O}$	$\gamma_{-T}\gamma_T$	w
9	$(S,-S)$	$\mathscr{O}$	$\gamma_S\gamma_{-S}$	u	20	$(-T,S+T)$	S	$\frac{\gamma_T\gamma_{-T}\gamma_{S+T}}{\gamma_S\gamma_T}$	vw
10	$(-S,S)$	$\mathscr{O}$	$\gamma_S\gamma_{-S}$	u	21	$(-T,-S+T)$	$-S$	$\frac{\gamma_{-T}\gamma_{-S+T}\gamma_S\gamma_T^3\gamma_{S+T}}{\gamma_{-S}\gamma_S\gamma_T^3\gamma_{S+T}}$	$\frac{wy}{uv\tau(d)}$
11	$(-S,-S)$	S	$\frac{\gamma_{-S}^3}{\gamma_S\gamma_{-S}}$	1					

We now use Lemma 3.4.6 to reduce the number of choices here down to just one unique choice. Because of the symmetry condition, we have $\rho(-T,T) = \rho(T,-T)$ and so $w = \tau(w)$, meaning that $w = 1$. We also have $\rho(-T,S+T) = \rho(S+T,-T)$ and so we find $vw = \sigma\tau(vw)$, so $v = \sigma\tau(v)$. This condition gives us $v = \frac{1}{\sigma^2(\xi)\tau\sigma(\xi)}$. From condition 3 of the lemma, we see that $\rho(S,S+T)\rho(-S+T,S+T) = \rho(S,-S-T)\rho(S+T,S+T)$, giving that $y = \frac{\sigma(v)\sigma\tau(d)}{\sigma\tau(v)}$. Summarizing, we get

$$v = \frac{1}{\sigma^2(\xi)\tau\sigma(\xi)} \qquad w = 1 \qquad y = 1.$$

Let us now simplify the coefficient of the $z_1^2 z_2$ term of (3.68).

$$\begin{aligned}\frac{\rho_{28}\rho_{11}}{\rho_{38}\rho_{55}} &= \frac{\rho(-S,-S-T)\rho(S,S)}{\rho(T,-S-T)\rho(-S+T,-S+T)} = \frac{\tau\sigma(uv)\cdot u\cdot\tau(v)du\cdot\sigma^2(w)}{\tau(wy)\cdot\tau\sigma(d)} \\ &= u\xi\,\tau(\xi).\end{aligned}$$

We can find the other coefficients to find the pushout form given as

$$\Xi z_0^3+\Pi(u^2z_1^3+uz_2^3)+\Upsilon z_0^2z_1+\Psi z_0z_1^2+\Phi z_0^2z_2+\Theta z_0z_2^2+\Lambda z_1^2z_2+\Gamma z_1z_2^2+\Omega z_0z_1z_2 \tag{3.74}$$

where

$$\begin{aligned}\Xi &= Tr_{M/L_1}\left(2\beta(\lambda_{57}-\lambda_{33})-c_3\left(2+\frac{1}{\tau(d)}\right)\right)\\ \Pi &= Tr_{M/L_1}\left(1+\frac{1}{2\tau(d)}\right)\\ \Upsilon &= 3Tr_{M/L_1}\left(\xi\,\tau(\xi)(\lambda_{28}-\lambda_{55})(\lambda_{22}-\lambda_{36})\right)\\ \Psi &= 3u^2Tr_{M/L_1}\left(\frac{1}{\xi\,\tau(\xi)}(\lambda_{16}-\lambda_{77}+\lambda_{22}-\lambda_{36})\right)\\ \Phi &= 3uTr_{M/L_1}\left(\frac{1}{\xi\,\tau(\xi)}(\lambda_{16}-\lambda_{77})(\lambda_{11}-\lambda_{38})\right)\\ \Theta &= 3Tr_{M/L_1}\left(\xi\,\tau(\xi)(\lambda_{28}-\lambda_{55}+\lambda_{11}-\lambda_{38})\right)\\ \Lambda &= 3uTr_{M/L_1}\left(\xi\,\tau(\xi)\right)\\ \Gamma &= 3u^2Tr_{M/L_1}\left(\frac{1}{\xi\,\tau(\xi)}\right)\\ \Omega &= -uTr_{M/L_1}\left(\lambda_{33}\left(2+\frac{1}{\tau(d)}\right)\right)\end{aligned} \tag{3.75}$$

All these coefficients lie in L_1, as required.

Example 3.5.3. Let $E: y^2 = x^3+(x+1)^2$, with Cremona reference $92a1$. Let ϕ be the isogeny with kernel generated by S, where

$$\begin{aligned}S &= (0,1)\\ T &= \left(\beta, \frac{\beta+3}{\sqrt{-3}}\right)\end{aligned}$$

and β satisfies $\beta^3+\frac{4}{3}\beta^2+4\beta+4=0$. A descent by 3-isogeny gives us that $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) = \langle 2\rangle$. We choose to use $u = 2\cdot 3^6$ because it gives a simpler pushout form. To construct a pushout form, we need

$$\begin{aligned}\xi &= \frac{9}{2}\beta^2\\ d &= \frac{1}{81}(-68\zeta_3-114)\beta^2+\frac{1}{27}(-80\zeta_3-24)\beta+\frac{1}{27}(-59\zeta_3+21)\end{aligned}$$

which we can fill in in the recipe in this section, giving us the covering curve

$$C_2: 2^2\cdot 3^{12}x^3+2^2\cdot 3^6xyz-2\cdot 3^6y^3+2z^3=0$$

and pushout form

$$\begin{aligned} f_1 =&(-2783322\zeta_3+16641612)x^3+2484432x^2y+(186624\zeta_3+268272)x^2z+279936xy^2\\ &+(22870\zeta_3+44992)xyz+(-1248\zeta_3-1380)xz^2+(-1909\zeta_3+11414)y^3\\ &+(1136\zeta_3+2470)y^2z+(-114\zeta_3+208)yz^2+\frac{1}{729}(-10177\zeta_3+7964)z^3. \end{aligned}$$

We see that

$$\begin{aligned} \operatorname{div}\left(\frac{f_1}{x^3}\right) =&3\cdot\left(\frac{1}{18978}(16848\zeta_3+6163)\gamma^2+\frac{1}{56934}(-1363\zeta_3-3248)\gamma+\frac{1}{56934}(-17\zeta_3-377):\gamma:1\right)\\ &-3\cdot(0:\frac{1}{9}:1)-3\cdot(0:\frac{1}{9}\zeta_3:1)-3\cdot(0:\frac{1}{9}(-\zeta_3-1):1) \end{aligned}$$

where $206769\gamma^3+(18357\zeta_3-7221)\gamma^2+(3158\zeta_3+391)\gamma+\frac{1}{81}(-5515\zeta_3-40295)=0$, showing f_1 is indeed a pushout form.

3.5.5 Generic 3-Isogeny

In this case, E if of the form (3.26) with $\Delta\neq 1,-3$. Consider $u\in S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$. Let $L_1=\mathbb{Q}(\sqrt{\Delta})$, $L_2=\mathbb{Q}(\sqrt{-3\Delta},\beta)$ and $M=\mathbb{Q}(\sqrt{-3},\sqrt{\Delta},\beta)$ where β is a root of $x^3+\frac{4}{3}\varepsilon^2\Delta x^2+4\varepsilon\eta\Delta x+4\eta^2\Delta$. Let G be the subgroup of G_K through which the action of G_K on $E[3]$ factors. We have $E[3]=\langle S,T\rangle$ where

$$\begin{aligned} \sigma(S)&=S & \tau(S)&=S & \delta(S)&=2S\\ \sigma(T)&=S+T & \tau(T)&=2T & \delta(T)&=2T. \end{aligned}$$

Let $\xi\in L_2$ be such that $N_{L_2/L_1}(\xi)=u$, and let $C\in\mathbb{Q}$ be such that $N_{L_1/\mathbb{Q}}(u)=C^3$. From Lemma 2.5.15 we obtain $d=\frac{\tau\sigma(\xi)\delta\sigma(\xi)\sigma(\xi)\delta\tau\sigma(\xi)}{\xi\delta\tau(\xi)\sigma\tau(\xi)\delta\sigma^2(\xi)}$ and the following holds. Note that $d=\delta\tau(d)$.

$$\begin{aligned} \alpha_1&=\delta(u) & \alpha_5&=\delta\sigma^2(d)\\ \alpha_2&=u & \alpha_6&=\sigma^2(d)\\ \alpha_3&=\delta(d) & \alpha_7&=\delta\sigma(d)\\ \alpha_4&=d & \alpha_8&=\sigma(d) \end{aligned}$$

Once again, we make ρ explicit, as explained in Section 3.4.1, the end of which tells us that there is a unique choice of ρ in this case. There are 13 orbits for the action of G_K on $E[3]\times E[3]$, with representatives listed in the following table. Recall that there exists $\gamma\in\overline{R}^\times$ with $\alpha=\gamma^3$ and $\rho=\partial\gamma$, and write γ_P for $\gamma(P)$. The column in the table labelled 'in γ' expresses the element $\rho(T_1,T_2)$ as a product of the γ_P. There are four choices to make, namely the following.

1. $t=\gamma_S\gamma_{-S}$, a cube root of $N_{L_1/\mathbb{Q}}(u)=C^3$.
2. $v=\frac{\gamma_{S+T}}{\gamma_S\gamma_T}$, a cube root of $\frac{\delta\sigma(d)}{\delta(u)\delta(d)}$.
3. $w=\gamma_T\gamma_{S+T}\gamma_{-S+T}$, a cube root of $N_{L_2/L_3}(\delta(d))=1$.
4. $y=\gamma_T\gamma_{-T}$, a cube root of $N_{L_2/L_4}(d)$.

#	(T_1,T_2)	T_1+T_2	in γ	ρ	#	(T_1,T_2)	T_1+T_2	in γ	ρ
1	$(\mathscr{O},\mathscr{O})$	$\mathscr{O}$	$\gamma_{\mathscr{O}}$	1	8	(S,T)	$S+T$	$\frac{\gamma_S\gamma_T}{\gamma_{S+T}}$	$\frac{1}{v}$
2	$(S,\mathscr{O})$	S	$\gamma_{\mathscr{O}}$	1	9	(T,S)	$S+T$	$\frac{\gamma_S\gamma_T}{\gamma_{S+T}}$	$\frac{1}{v}$
3	$(T,\mathscr{O})$	T	$\gamma_{\mathscr{O}}$	1	10	(T,T)	$-T$	$\frac{\gamma_T^3}{\gamma_T\gamma_{-T}}$	$\frac{\delta(d)}{y}$
4	$(\mathscr{O},S)$	S	$\gamma_{\mathscr{O}}$	1	11	$(-T,T)$	$\mathscr{O}$	$\gamma_T\gamma_{-T}$	y
5	$(\mathscr{O},T)$	T	$\gamma_{\mathscr{O}}$	1	12	$(S+T,-S+T)$	$-T$	$\frac{\gamma_{S+T}\gamma_{-S+T}\gamma_T}{\gamma_{-T}\gamma_T}$	$\frac{w}{y}$
6	(S,S)	$-S$	$\frac{\gamma_S^3}{\gamma_S\gamma_{-S}}$	$\frac{\delta(u)}{t}$	13	$(S+T,-T)$	S	$\frac{\gamma_T\gamma_{S+T}\gamma_{-T}}{\gamma_S\gamma_T}$	vy
7	$(S,-S)$	$\mathscr{O}$	$\gamma_S\gamma_{-S}$	t					

We use Lemma 3.4.6 to reduce the choices here. By the symmetry condition, we have $\rho(S,-S) = \rho(-S,S)$, therefore $t = \delta(t)$ and $t = \tau(t)$, and we must have $t = C$. We also have $\rho(-T,T) = \rho(T,-T)$, and so $y = \tau(y)$. From $\rho(S+T,-T) = \rho(-T,S+T)$, giving us $vy = \sigma\tau(vy)$. Finally, we have $\rho(S+T,-S+T) = \rho(-S+T,S+T)$, thus $\frac{w}{y} = \frac{\delta\tau(w)}{\delta\tau(y)}$. These conditions ensure that we must make the following choices.

$$t = C \qquad v = \frac{C\sigma^2(\xi)\tau(\xi)}{u\delta\sigma(\xi)\delta\tau\sigma(\xi)} \tag{3.76}$$

$$w = 1 \qquad y = \frac{\tau\sigma(\xi)\delta\sigma(\xi)\sigma(\xi)\delta\tau\sigma(\xi)}{C^2} \tag{3.77}$$

The covering curve associated to u can be obtained from (3.55).

$$C_u : \delta(u)z_1^3 - uz_2^3 + 2\eta\sqrt{\Delta}z_0^3 + 2\varepsilon C\sqrt{\Delta}z_0z_1z_2 = 0 \tag{3.78}$$

As we did in earlier sections, we can now rewrite the pushout form from (3.68) as follows

$$\Xi z_0^3 + \Pi\left(\delta(u)z_1^3 + uz_2^3\right) + \Phi z_0^2z_1 + \delta\tau(\Phi)z_0^2z_2 + \Psi z_0z_1^2 + \delta\tau(\Psi)z_0z_2^2 + \Upsilon z_1^2z_2 + \delta\tau(\Upsilon)z_1z_2^2 + \Omega z_0z_1z_2 \tag{3.79}$$

where $H = \frac{\delta\tau(\xi)\delta\sigma^2(\xi)}{\xi\sigma\tau(\xi)}$ and

$$\Xi = Tr_{M/M'}\left(2\beta(\lambda_{57}-\lambda_{33}) - c_3\left(2+\frac{1}{\delta(d)}\right)\right) \tag{3.80}$$

$$\Pi = Tr_{M/M'}\left(1+\frac{1}{2\delta(d)}\right) \tag{3.81}$$

$$\Phi = \frac{3u}{C}Tr_{M/M'}\left(H\cdot(\lambda_{26}-\lambda_{33})(\lambda_{22}-\lambda_{47})\right) \tag{3.82}$$

$$\Psi = \frac{3C\delta(u)}{u}Tr_{M/M'}\left(\frac{1}{H}\cdot(\lambda_{16}-\lambda_{77}+\lambda_{22}-\lambda_{36})\right) \tag{3.83}$$

$$\Upsilon = 3uTr_{M/M'}(H) \tag{3.84}$$

$$\Omega = -CTr_{M/M'}\left(\lambda_{33}\left(2+\frac{1}{\delta(d)}\right)\right) \tag{3.85}$$

Via the substitution

$$z_0 = Z$$
$$z_1 = X + \sqrt{\Delta}Y$$
$$z_2 = X - \sqrt{\Delta}Y$$

we obtain a covering curve over $\mathbb{Q}$ and a pushout form over $\mathbb{Q}(\sqrt{-3\Delta})$.

Example 3.5.4. Let E be the elliptic curve given by

$$E : y^2 = x^3 + 2(x+1)^2$$

where $E[3] = \langle S, T\rangle$ with $S = (0, -\sqrt{2})$ and $T = (\beta, \sqrt{2}\left(-\frac{1}{3}\beta^2 + (-\frac{1}{3}\zeta_3 - \frac{5}{9})\beta + \frac{10}{9}\zeta_3 - \frac{7}{9}\right))$, with β satisfying $\beta^3 + \frac{8}{3}\beta^2 + 8\beta + 8 = 0$. Then E admits an isogeny $\phi : E \to \hat{E}$ of degree 3, with kernel $\langle S\rangle$. We obtain the Selmer group $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) = \langle -1+\sqrt{2}\rangle \subset \mathbb{Q}(\sqrt{2})^\times/(\mathbb{Q}(\sqrt{2})^\times)^3$. Let $M = \mathbb{Q}(\beta)$, and we find ξ such that $N_{M/\mathbb{Q}(\sqrt{2})}(\xi) = -1+\sqrt{2}$. We find $\xi = \frac{1}{2}(18\sqrt{2}+27)\beta^2 + (15\sqrt{2}+15)\beta + 61\sqrt{2} + 77$. Then the covering curve associated to $-1+\sqrt{2}$ found using (3.78) is given by

$$C_{-1+\sqrt{2}} : -2x^3 - 6x^2y - 2x^2z - 12xy^2 - 4y^3 + 4y^2z + 2z^3 = 0$$

and the pushout form is given by

$$\begin{aligned} f_1 =& (1140\sqrt{-6} - 1879)x^3 + (6840\sqrt{-6} - 7962)x^2y + (1417\sqrt{-6} - 7072)x^2z + (6840\sqrt{-6} - 7866)xy^2 \\ &+ (1072\sqrt{-6} + 2376)xyz + (-136\sqrt{-6} + 1228)xz^2 + (4560\sqrt{-6} - 7324)y^3 + (-1258\sqrt{-6} + 18080)y^2z \\ &+ (140\sqrt{-6} - 1552)yz^2 + 1/9(-47153\sqrt{-6} + 17784)z^3. \end{aligned}$$

We see that

$$\begin{aligned} \operatorname{div}\left(\frac{f_1}{x^3}\right) =& 3\cdot\left(\frac{1}{34925}(-30872\sqrt{-6} - 43936)\alpha_1^2 + \frac{1}{104775}(25441\sqrt{-6} - 89592)\alpha_1\right. \\ &\left. + \frac{1}{104775}(17371\sqrt{-6} - 149152) : \alpha_1 : 1\right) - 3\cdot(0 : \alpha_2 : 1) \end{aligned}$$

where $492768\alpha_1^3 + (11664\sqrt{-6} - 9864)\alpha_1^2 + (-178008\sqrt{-6} + 97560)\alpha_1 + 16424\sqrt{-6} + 135897 = 0$ and $\alpha_2^3 - \alpha_2^2 - \frac{1}{2} = 0$, showing that f_1 is indeed a pushout form.

3.6 Other Methods of Computing Pushout Forms

In this section we take a different approach to finding pushout forms, which can also be used to simplify pushout forms already calculated. This method is used in Chapter 7.

Let $C \subset \mathbb{P}^{n-1}$ be a genus 1 normal curve of degree n defined over a number field K and assume that C is everywhere locally soluble. Let E be the Jacobian of C, and as before we have an isomorphism sum: $\mathrm{Pic}^0(C) \cong E$. The *hyperplane section* of C is a degree n effective K-rational divisor H on C, defined up to linear equivalence. Solving the following problem for a certain point P is equivalent to finding a pushout form on C.

Problem 3.6.1. *Given $C \subset \mathbb{P}^{n-1}$ a genus 1 normal curve of degree n with hyperplane section H, and a point $P \in E(K)$, find equations for an embedding $C \hookrightarrow \mathbb{P}^{n-1}$ whose image is a genus 1 normal curve of degree n with hyperplane section H' such that sum$(H' - H) = P$.*

Recall the construction of a pushout form given in the discussion prior to Definition 3.3.1. Let $\mathcal{O} \neq \hat{S} \in \hat{E}[n]$, $D_{\hat{S}}$ a divisor corresponding to $\hat{S}$ under sum: $\mathrm{Pic}^0(\hat{E}) \cong \hat{E}$ and extend K to include the coordinates of $\hat{S}$. Then we saw that there exists $f_{\hat{S}} \in K(\hat{E})$ with $\operatorname{div}(f_{\hat{S}}) = n\cdot D_{\hat{S}}$. By solving Problem 3.6.1 with $P = \hat{T}$, we obtain $D_{\hat{S}}$ in the form $H' - H$, which allows us to compute $f_{\hat{S}}$. Denote by $K[x_1, \ldots, x_n]_d$ the space of

homogeneous polynomials of degree d, and let $\mathscr{L}(A)$ be the Riemann-Roch space for a divisor A. From [BL04, Theorem 7.3.1], we have that for any $d \geq 1$ the following map is surjective

$$\begin{aligned} K[x_1,\ldots,x_n]_d &\longrightarrow \mathscr{L}(d\cdot H) \\ f &\longmapsto \frac{f}{g(x_1,\ldots,x_n)^d} \end{aligned}$$

where g is a linear form corresponding to H. Letting $d = n$, and assuming that $H = C \cap \{x_1 = 0\}$, we can write f in the form f_1/x_1^n where f_1 is a degree n form meeting C in divisor $n\cdot H'$.

In the case that C is a smooth plane cubic and $n = 3$, a solution to Problem 3.6.1 is given in [FN14] of which we give a brief overview. The curve C can be embedded into $\mathbb{P}^2$ using either the linear system $|H|$ or the linear system $|H'|$. Using both embeddings gives a map

$$C \longrightarrow \mathbb{P}^2 \times \mathbb{P}^2$$

whose image is defined by three bi-homogeneous forms of degree $(1,1)$. The coefficients can be put into a $3\times 3\times 3$ cube. By observing that this cube consists of three 3×3 matrices M_1, M_2 and M_3, we then have the following ternary cubic.

$$F(x,y,z) = \det(xM_1 + yM_2 + zM_3) \tag{3.86}$$

By slicing the cube in three different ways, we obtain three different such ternary cubics. It can then be shown, as is done in [Ng95, Theorem 1], that two of these define the image of C under the embeddings corresponding to H and H', and an isomorphism between these plane cubics is given by the 2×2 minors of the matrix of linear forms in (3.86). Thus we are in the case of Problem 3.6.1 and can compute a pushout form. The goal therefore becomes to compute suitable matrices M_1, M_2, M_3. Unfortunately, this method does not seem to generalise to any case with $n > 3$, as it relies on many properties of such $3\times 3\times 3$ cubes, therefore we will not pursue it here and refer to [FN14] for details.

This method can also be used to simplify pushout forms already obtained. Say that we have some pushout form f with $\operatorname{div}(f) = n\cdot A$. Then we may replace f with f' having $\operatorname{div}(f') = n\cdot A'$, if we have A linearly equivalent to A'. Explicitly, we follow the following method. Let E be an elliptic curve, $\phi : E \to \hat{E}$ an isogeny of degree n, and $C \subset \mathbb{P}^{n-1}$ a covering curve corresponding to some element of the Selmer group $S^{(\phi)}(E/K)$. Assume we have some pushout form f_1 such that $\frac{f_1}{x_1^n} \in K(C)$. Then $\operatorname{div}\left(\frac{f_1}{x_1^n}\right) = n\cdot H_f - n\cdot H$ with $n\cdot H_f$ and $n\cdot H$ linearly equivalent divisors. We will be seeking some new divisor H_g, which must be linearly equivalent to H_f, and will be simpler than H_f.

We have the standard embedding

$$\upsilon : C \xhookrightarrow{|H_f|} \mathbb{P}^{n-1}.$$

given by $\upsilon = (\upsilon_1,\ldots,\upsilon_n)$. In MAGMA, this embedding is given by the function `DivisorMap`. Each υ_i is given by a homogeneous polynomial of degree n in the variables $x_1,\ldots,x_n$. Let N be the number of monomials of degree n. Then we have

$$\upsilon_i = \chi_{i,1}x_1^n + \chi_{i,2}x_1^{n-1}x_2 + \chi_{i,3}x_1^{n-1}x_3 + \ldots + \chi_{i,N}x_n^n.$$

Then we can construct the $n\times N$ matrix of coefficients $M = (\chi_{i,j})_{i\in\{1,\ldots n\},j\in\{1\ldots N\}}$. This matrix corresponds to a lattice L of dimension n and degree N with basis the rows of M and standard Euclidean inner

product. We can now use all available methods to simplify the basis of this lattice. For example, we used MAGMA's `PureLattice` to find the pure lattice $L_{\text{new}} = (\mathbb{Q} \otimes L) \cap \mathbb{Z}^n$, which generates the same subspace in $\mathbb{Q}^n$ as L, but has a simpler basis matrix. We can further reduce this basis by using the LLL algorithm [LLL82].

The new basis of L corresponds to a different embedding of $\Upsilon : C \hookrightarrow \mathbb{P}^{n-1}$. Let M_{new} be the matrix with rows the new basis vectors of L, so we have $M_{\text{new}} = (\omega_{i,j})_{i \in \{1,\ldots n\}, j \in \{1 \ldots N\}}$. Thus $\Upsilon = (\Upsilon_1, \ldots, \Upsilon_n)$ where

$$\Upsilon_i = \omega_{i,1} x_1^n + \omega_{i,2} x_1^{n-1} x_2 + \omega_{i,3} x_1^{n-1} x_3 + \ldots + \omega_{i,N} x_n^n.$$

This new embedding corresponds to some divisor H_g which is linearly equivalent to H_f. Thus $n \cdot H_g$ and $n \cdot H$ are also linearly equivalent and we can find, using the MAGMA function `IsLinearlyEquivalent`, some $g \in \mathscr{L}(n \cdot H)$ such that $n \cdot H_g = n \cdot H + \operatorname{div}(g)$. We have found a new pushout form g, which should be simpler than f because it corresponds to a simpler and more attractive basis for the lattice L. We may simplify g further if necessary, by adding or subtracting multiples of the equation of C, which of course does not alter the divisor of g.

We finish this chapter by continuing Example 3.5.2, and simplifying the pushout forms found there. In Chapter 7, we describe a new way to solve Problem 3.6.1 for $P \in E[3]$ and use the solution to turn a 3-descent into a 3ϕ-descent.

Example 3.6.2. We now continue Example 3.5.2 from the previous section. Recall that we had found some pushout forms, but they had rather large coefficients. We now employ the tactics discussed in this section to simplify them further.

For every pushout form f_1 from Example 3.5.2, we have that $\operatorname{div}\left(\frac{f_1}{x^3}\right) = 3 \cdot H_f - 3 \cdot H$. The following table gives H_f, as well as some linearly equivalent divisor H_g, which we found by the procedure given above.

$S^{(\hat{\phi})}(\hat{E}/K)$	H_f	H_g
ζ_3	$\left(\frac{1}{181}(111\alpha^2 - 42\alpha - 1568) : \alpha : 1\right)$	$\left(\beta^2 + 4\beta - 4 : \beta : 1\right)$
$-14\zeta_3 + 7$	$\left(\frac{1}{711671}(-1294842\gamma^2 + 337764\gamma + 2523106) : \gamma : 1\right)$	$\left(4\delta^2 - 6\delta - 2 : \delta : 1\right)$

where we have

$$111\alpha^3 - 36\alpha^2 - 2397\alpha + 62 = 0 \qquad \beta^3 + 4\beta^2 - 11\beta + 10 = 0$$
$$3884526\gamma^3 + 2043\gamma^2 - 11353386\gamma - 1977814 = 0 \qquad 8\delta^3 - 10\delta^2 - 6\delta - 1 = 0.$$

We obtain the following new pushout forms by following the procedure outlined above.

$S^{(\hat{\phi})}(\hat{E}/K)$	pushout forms
ζ_3	$x^3 + 36x^2y + 224x^2z - 339xy^2 + 414xyz - 806xz^2 - 734y^3 - 66y^2z + 4350yz^2 - 44z^3$
$-14\zeta_3 + 7$	$264x^3 - 423x^2y + 372x^2z + 399xy^2 - 1200xyz + 280xz^2 + 178y^3 - 204y^2z - 480yz^2 + 348z^3$

In bigger examples, the reduction in coefficient size is often more dramatic than in this small example.

Chapter 4

Improving Norm Equation Calculations

Let K be a number field and L/K a cubic field extension. Let O_K be the ring of integers of K. To calculate pushout forms, there are norm equations to solve of the form

$$N_{L/K}(\xi) = x \tag{4.1}$$

where x is some element of K and $\xi \in L$ is to be determined. The computer algebra software package MAGMA [BCP97] has an inbuilt function `NormEquation` to solve such equations using a method described in [Coh00, Section 7.5] and [Sim02]. This method involves computing a set of primes S consisting of the primes dividing the ideal xO_K together with the primes generating the relative class group $Cl(L/K)$. Computing the class group can be a very laborious thing to do if the discriminant of L is large. In this chapter, we discuss modifications made to improve these calculations based on methods from [Cas71].

In this chapter, we will be encountering many cubic extensions, so we quickly recall an important fact about cubic field extensions here. Assume we have a cubic extension of K given by $L = K(\sqrt[3]{b})$ with $b \in K$. Then we can represent any element of L in the following manner.

$$A + B\sqrt[3]{b} + C\sqrt[3]{b}^2 = \frac{\alpha + \beta\sqrt[3]{b}}{\gamma + \delta\sqrt[3]{b}} \tag{4.2}$$

$$\alpha = AB - C^2 b \qquad \beta = B^2 - AC$$
$$\gamma = B \qquad \delta = -C$$

This works unless $B = C = 0$, which is of course a trivial case. The idea in this chapter is to change the problem such that we are computing norms over smaller cubic extensions. The method will closely resemble that used in [CR02] in which solutions are sought to conics of the form

$$X^2 - aZ^2 = bY^2. \tag{4.3}$$

Assuming $|a| < |b|$, we find a solution (x_0, z_0) to $X^2 - aZ^2 \equiv 0 \pmod{b}$ such that $x_0^2 + |a|z_0^2$ is as small as possible. We then set $t = \frac{x_0^2 - az_0^2}{b}$, and write $t = t_1 t_2^2$ with t_1 squarefree. Under certain conditions, we will

have $|t_1| < |b|$ and if (x_1, y_1, z_1) is a solution to $X^2 - aZ^2 = t_1 Y^2$, then

$$(x, y, z) = (x_0 x_1 + a z_0 z_1, t_1 t_2 y_1, z_0 x_1 + x_0 z_1)$$

will be a solution to (4.3). This process can then be iterated, swapping the roles of a and b if necessary to ensure $|a| < |b|$. We will see in this chapter how this process can be adapted for our purposes.

4.1 Basic Concepts of Reduction

Let $K = \mathbb{Q}$. This section is concerned with finding small solutions to binary cubic polynomials. To do so, we recall the concept of a reduced form. Following the same procedure as is laid out in [Cre99] we define the concept of reduction in the case of binary quadratic polynomials. We then define the concept of a reduced form in the binary cubic case by associating a quadratic form to every cubic form and defining the cubic to be reduced if the quadratic is.

Let F be some binary quadratic form in $\mathbb{R}[X, Y]$, and $\Delta(F)$ its discriminant.

$$\begin{aligned} F(X, Y) &= aX^2 + bXY + cY^2 \\ \Delta(F) &= b^2 - 4ac \end{aligned} \tag{4.4}$$

The group $SL_2(\mathbb{Z})$ acts on $\mathbb{R}[X, Y]$ via

$$F(X, Y) \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = F(\alpha X + \beta Y, \gamma X + \delta Y).$$

The discriminant $\Delta(F)$ is invariant under this action. It will sometimes be convenient to associate to the homogeneous polynomial F the inhomogeneous polynomial $f(X) = F(X, 1) = aX^2 + bX + c$.

Definition 4.1.1. The binary quadratic polynomial (4.4) is *positive definite* if $a > 0$ and $\Delta(F) < 0$.

If F is positive definite, then the roots of the polynomial $f(X) = F(X, 1)$ must be a pair of complex conjugates $z, \overline{z}$, one of which lies in the upper half plane

$$H = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}.$$

A positive definite form F remains positive definite under the action of $SL_2(\mathbb{Z})$. Thus we can speak of an orbit of F under this action.

Definition 4.1.2. The form $F(X, Y) = aX^2 + bXY + cY^2$ is *reduced* if

$$|b| \leq a \leq c. \tag{4.5}$$

Equivalently, F is reduced if its root z lies in the fundamental region

$$\mathscr{F}_{\mathbb{Q}} = \left\{ z \mid z \in H,\ |z| \geq 1,\ -\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2} \right\}.$$

Thus to every positive definite quadratic form $F(X, Y)$, we can associate a point in the upper half plane, namely its root z. The action of $SL_2(\mathbb{Z})$ on H is generated by the elements

$$M_\times = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad\qquad M_\omega = \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}$$

for $\omega \in \mathbb{Z}$. Every positive definite form is equivalent to a reduced form under this action. This reduced form is unique unless one of the inequalities in (4.5) is an equality, in which case there are two reduced forms differing only in the sign of b. Of course, we can eliminate this ambiguity by demanding $b > 0$ in this case.

We now consider a binary cubic form

$$F(X,Y) = aX^3 + bX^2Y + cXY^2 + dY^3. \tag{4.6}$$

We want to define a notion of 'reduced' as in the quadratic case. The only invariant of F is the discriminant

$$\Delta(F) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

We now proceed differently, depending on the sign of $\Delta(F)$. If $\Delta(F) > 0$, we follow [Cre99]. By considering the Hessian matrix of F, we are naturally led to consider the Hessian covariant

$$h(X) = (b^2 - 3ac)X^2 + (bc - 9ad)X + (c^2 - 3bd).$$

Unless $\Delta(F) > 0$, $h(X)$ is not definite. In the following sections, we will have to consider only binary cubics with negative discriminant, therefore the Hessian will not be an appropriate quadratic form to associate to F and this is the last time we shall see it in this thesis.

If $\Delta(F) < 0$, then F has one real root α and a pair of complex roots $\beta, \overline{\beta}$. Following Belabas [Bel97], and Mathews and Berwick [Mat12] we define the positive definite form

$$Q(F) = (X - \beta)(X - \overline{\beta}). \tag{4.7}$$

There are other forms we could choose, some of which are discussed in [Cre99], however this is the simplest option, and is sufficient for our purposes. We are led to the following definition.

Definition 4.1.3. A binary cubic form (4.6) is *Minkowski-reduced* if the positive definite form $Q(F)$ in (4.7) is reduced in the sense of Definition 4.1.2.

Various other notions of 'reduced' have been used. Cremona [Cre99] and Julia [Jul17] use the following covariant of F

$$J_2(X) = h_0X^2 + h_1X + h_2$$

where

$$\begin{aligned} h_0 &= 9a^2\alpha^2 + 6ab\alpha + 6ac - b^2 \\ h_1 &= 6ab\alpha^2 + 6(b^2 - ac)\alpha + 2bc \\ h_2 &= 3ac\alpha^2 + 3(bc - 3ad)\alpha + 2c^2 - 3bd \end{aligned}$$

which leads to an improved bound on $|a|$ in the reduced cubic.

Recall that we are interested in the reduction of binary cubics in so far as it allows us to compute small solutions. Thus we are led to consider the following, proved by Davenport in 1945 [Dav45].

Theorem 4.1.4 ([Cas71, Section II.5.4, Theorem IX])**.** *If $f(X,Y)$ is a binary cubic form with discriminant $D = \Delta(f) < 0$, then there are integers $(U,V) \neq (0,0)$ such that*

$$|f(U,V)| \leq \left|\frac{D}{23}\right|^{\frac{1}{4}}.$$

If, further, $f(X,Y)$ is Minkowski-reduced in the sense of Definition 4.1.3, then

$$\min\{|f(1,0)|,|f(0,1)|,|f(1,-1)|,|f(1,-2)|\} \leq \left|\frac{D}{23}\right|^{\frac{1}{4}},$$

with equality only when

$$f(X,Y) = A(X^3+X^2Y+2XY^2+Y^3).$$

Thus by reducing a cubic form, we can easily find a point such that the form evaluated at that point satisfies a certain useful upper bound.

4.2 Improving the Norm Equation in the Case $K = \mathbb{Q}$

Let $K = \mathbb{Q}$. Say that we have $a,b \in \mathbb{Z}$ such that we know there exists $\xi \in \mathbb{Q}(\sqrt[3]{b})$ such that $N_{\mathbb{Q}(\sqrt[3]{b})/\mathbb{Q}}(\xi) = a$. This section will be concerned with how to compute this element ξ without resorting to the MAGMA function `NormEquation`. The goal will be to change the norm equation to be solved into one with smaller a and b, thus making it simpler. In this case, we will show that in fact we can reduce to the case $|a| = 1$.

Let ξ be given in the form $\frac{\alpha+\beta\sqrt[3]{b}}{\gamma+\delta\sqrt[3]{b}}$. Then

$$a = N_{\mathbb{Q}(\sqrt[3]{b})/\mathbb{Q}}(\xi) = \frac{\alpha^3+b\beta^3}{\gamma^3+b\delta^3}$$

from which it follows that

$$a\gamma^3 + ab\delta^3 = \alpha^3 + b\beta^3 \tag{4.8}$$

and so we obtain

$$V_{a,b} = \{x_1^3 + ax_2^3 + bx_3^3 + abx_4^3 = 0\} \subset \mathbb{P}^3 \tag{4.9}$$

which must contain a point over $\mathbb{Q}$.

Theorem 4.2.1. *Let $a,b \in \mathbb{Z}$. Then the following are equivalent*

1. *a is a norm for $\mathbb{Q}(\sqrt[3]{b})/\mathbb{Q}$.*
2. *b is a norm for $\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}$.*
3. *a^2b is a norm for $\mathbb{Q}(\sqrt[3]{a+b})/\mathbb{Q}$.*
4. *a^2b is a norm for $\mathbb{Q}(\sqrt[3]{a-b})/\mathbb{Q}$.*
5. *$V_{a,b}(\mathbb{Q}) \neq \emptyset$.*

Proof. We have already shown that 1 and 5 are equivalent by the calculation (4.8), unless $\gamma = \delta = 0$. We see from (4.2) that this only happens when a is a perfect cube in $\mathbb{Q}$, which is a trivial case. The symmetry in 5 also shows that 2 and 5 are equivalent.

We now prove that 3 is equivalent to 2. First let b be a norm for $\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}$. We know that $\frac{a+b}{a} = 1+\frac{b}{a}$ is a norm for $\mathbb{Q}(\sqrt[3]{\frac{b}{a}})/\mathbb{Q}$. Using the equivalence of 1 and 2, we see that a is a norm for $\mathbb{Q}(\sqrt[3]{\frac{b}{a}})/\mathbb{Q}$ if and

only if $\frac{b}{a}$ is a norm for $\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}$. We are assuming that b is a norm for $\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}$ and of course a is trivially a norm in this extension. Thus a is norm for $\mathbb{Q}(\sqrt[3]{\frac{b}{a}})/\mathbb{Q}$ giving us that $a+b$ is as well, meaning that $\frac{b}{a}$ is a norm for $\mathbb{Q}(\sqrt[3]{a+b})/\mathbb{Q}$, as required. The converse is given by following this construction in the opposite direction. A very similar argument can be made using $a-b$ instead of $a+b$, thus giving us that 4 is also equivalent to 2. □

Theorem 4.2.1 is the first ingredient in our norm equation calculation. The next ingredient relies on the theory presented in Section 4.1. We will create a binary cubic form with suitable properties along the same lines as was done in [CR02] for binary quadratics.

Using Theorem 4.2.1, we can swap over the roles of a and b. Without loss of generality, assume that $|a| < |b|$, and let $b = b_1 b_2^2$ with b_1 squarefree. Assume both a and b are cubefree. Let p be a prime divisor of b_1. We know that if $V_{a,b}$ in (4.9) has a global solution, it must surely also have a local solution over $\mathbb{Q}_p$. Such a local solution would satisfy the equation $x_1^3 + ax_2^3 = 0 \pmod{p}$. If $x_2 = 0 \pmod{p}$, then we also have $x_1 = 0 \pmod{p}$. Substituting $b = pb'$, $x_1 = px_1'$ and $x_2 = px_2'$ into (4.9), we find

$$p^2(x_1')^3 + ap^2(x_2')^3 + b'x_3^3 + ab'x_4^3 = 0 \pmod{p}$$

and so we have $x_3^3 + ax_4^3 = 0 \pmod{p}$. We can repeat this argument until we have some $x_i^3 + ax_j^3 = 0 \pmod{p}$ but $x_j \neq 0 \pmod{p}$. Thus there exists $c_p \in \mathbb{Z}$ such that $a \equiv c_p^3 \bmod p$ for each such p. The Chinese Remainder Theorem then gives us $c \in \mathbb{Z}$ such that $a \equiv c^3 \bmod b_1$, which we need for the following construction.

Consider the following form with integer coefficients

$$F(X,Y) = \frac{1}{b_1}\left((cX + b_1Y)^3 - aX^3\right) \in \mathbb{Z}[X,Y] \tag{4.10}$$

which has discriminant $\Delta(F) = -27a^2b_1^2$. This discriminant is always negative, which allows us to use the theory from the previous section, and in particular Theorem 4.1.4. Thus there exist coprime $U,V \in \mathbb{Z}$ such that

$$|F(U,V)| \leq \left(\frac{27}{23}\right)^{\frac{1}{4}} |a|^{\frac{1}{2}} |b_1|^{\frac{1}{2}}. \tag{4.11}$$

We observe that

$$\begin{aligned} N_{\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}}(b_2((cU + b_1V) - \sqrt[3]{a}U)) &= b_1 b_2^3 F(U,V) \\ &= bb_2 F(U,V). \end{aligned}$$

The norm is multiplicative, so if we can find some element η such that $N_{\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}}(\eta) = b_2F(U,V)$ we will have found ξ such that $N_{\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}}(\xi) = b$.

Of course, ideally we want $|b_2F(U,V)| < |b|$ or this procedure does not help us reduce the size of b. Using (4.11), it would therefore suffice to have

$$\sqrt{\frac{27}{23}}|a| < |b|.$$

The following algorithm can now be used to solve a norm equation.

Algorithm 4.2.2. ***Input:*** *Two positive integers a,b such that b is a norm for $\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}$.*
Output: *A list of elements (a,b) at each iterative step such that b is a norm for $\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}$ and $|a_{\text{new}}| \leq a$.*
Initialization: *If $a = c^3a'$ for some c, let $a \leftarrow a'$. If $b < a$, swap the roles of a and b to ensure $|a| < |b|$. Then iterate the following steps.*

1. *If $b = c^3b'$ for some c, let $b \leftarrow b'$.*
2. *Create the binary cubic form F from* (4.10).
3. *Reduce F to some F_{red} by associating it to a positive definite form $Q(F)$ from* (4.7).
4. *Use the second part of Theorem 4.1.4 to find a minimizing $U_{\text{red}}, V_{\text{red}}$ of F_{red}.*
5. *Find (U,V), the minimizing point of F from $(U_{\text{red}}, V_{\text{red}})$.*
6. *If $|b_2F(U,V)| < |b|$, let $a_{\text{new}} \leftarrow a$ and $b_{\text{new}} \leftarrow b_2F(U,V)$. Else let $a_{\text{new}} \leftarrow |b| - |a|$ and $b_{\text{new}} \leftarrow a^2b$, which implements 3 and 4 from Theorem 4.2.1.*
7. *If $b_{\text{new}} < a_{\text{new}}$ then set $a \leftarrow b_{\text{new}}$ and $b \leftarrow a_{\text{new}}$. Else let $a \leftarrow a_{\text{new}}$ and $b \leftarrow b_{\text{new}}$.*

Repeat until $|a| = 1$.

If we keep track of all manipulations of a and b throughout this algorithm, we can then reconstruct a suitable element to solve the norm equation $N_{\mathbb{Q}(\sqrt[3]{b})/\mathbb{Q}}(\xi) = a$.

It does not seem a simple matter to give a rigorous complexity result, even if we assume that we always have $\sqrt{\frac{27}{23}}|a| < |b|$ at each step and that therefore we always have $|b_2F(U,V)| < |b|$ in step 6 of the algorithm. All we can guarantee in that case is that the new b will be smaller than the old b, but nothing further about the speed at which it decreases. We can however prove the following weaker result.

Theorem 4.2.3. *Algorithm 4.2.2 always terminates.*

Proof. We prove this theorem by showing that $|a|$ must always reduce to 1. Every iteration, there are three possibilities for what happens to a.

1. a gets swapped with b. This only happens if $|b| < |a|$, therefore this reduces $|a|$.
2. $|a|$ reduces but $|b|$ increases. This can only happen if $\sqrt{\frac{27}{23}}|a| \geq |b| > |a|$ and no suitable U,V were found in step 4. We then get $|a_{\text{new}}| = |b| - |a| \leq \frac{\sqrt{27}-\sqrt{23}}{\sqrt{23}}|a| < |a|$.
3. $|a|$ stays the same. This happens when step 5 is successful, but $|b_{\text{new}}| > |a|$. This cannot happen every iteration as then we would always have b decreasing but never being smaller than $|a|$. Within a finite number of steps we must end up in one of the previous cases.

□

The following examples show the reduction process in action. The first example is also small enough to show the solution to the norm equation we obtained using this method.

Example 4.2.4. Let $a = 5115287721793$ and $b = 99954$. Running our algorithm gives the following iterations.

Iteration	a	b	c	U	V
1	5115287721793	99954			
2	5115287721793	3702			
3	3702	5115287721793	2399117156730	-355138	166563
4	3702	31329471	27262989	-886	771
5	3702	167665	25153	20	-3
6	3702	-175			
7	-175	3702	3671	-1	1
8	-175	8			
9	-175	1			
10	1	-175			

By keeping track each step of the way, we thus find that $N_{\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}}\left(\frac{u+v\sqrt[3]{a}}{w+y\sqrt[3]{a}}\right) = b$ where

$$u = 28002397299114135 \qquad v = 4553858177529$$
$$w = -239644398893060 \qquad y = 99680056606$$

Example 4.2.5. Let $a = 475943754398$ and $b = 144974372703916041375620 43$. Of course, we would not want to compute class groups or units in either $\mathbb{Q}(\sqrt[3]{a})$ or $\mathbb{Q}(\sqrt[3]{b})$, since MAGMA fails to compute these at all in this case. Running our algorithm gives the following iterations. In this case, for the sake of brevity we have left out the steps swapping the roles of a and b or removing cubes until the final few steps.

Iteration	a	b	c	U	V
1	475943754398	144974372703916041375620 43	13040996527027402990871081	-22566991816	20299867929
2	475943754398	1305019405624780313	562103019023909274	8920801	-3842402
3	475943754398	-203142301070862	124241776114472	52984	32405
4	475943754398	1176907695860	126982936082	-3939	1700
5	177059691796	475943754398	397192350374	-1801	1503
6	135001895302	177059691796	106344009	133	-54
7	135001895302	-31559584862	10741940314	-379	-129
8	22345195257	135001895302	117731257899	5847	-5099
9	22345195257	-33082287218	12577646905	-3009	-1144
10	-2202230654	22345195257	22961431	-64	29
11	-949205271	-2202230654	273883861	394	49
12	-402541684	-949205271	593561816	-387	-242
13	-402541684	464089212	4082573	60	-19
14	43371174	-402541684	61403307	-59	-36
15	-10368786	43371174	791616	19	-17
16	-1547861	-10368786	1847347	174	31
17	-807372	-1547861	14706	-15	-7
18	570269	-807372	13694	5	3
19	-53829	570269	318431	77	-43
20	19453	-53829	4311	7	5
21	-6747	19453	53	1	0
22	-6747	2744			
23	-6747	1			
24	1	-6747			

In this case, the solution is simply too large to present here, however running the algorithm takes very much less time than a second, thus clearly an improvement. In this thesis, we are not overly concerned

with the size of the solutions we obtain via this method, however this would definitely be a point to improve on.

The following table gives a comparison between our method and the standard one implemented in MAGMA. It is not intended as anything other than a rough indication of how useful this method is practically speaking. We use version 2.21-1 of MAGMA. Initial values for a and b were randomly generated as follows. We randomly selected any $a, b_0, b_1, b_2 \in \mathbb{Z}$ using MAGMA's `Random` function, and let $b = N_{\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}}(b_0 + b_1\sqrt[3]{a} + b_2\sqrt[3]{a^2})$. We always ensured that $|a| < |b|$, swapping their roles if necessary to achieve this, and then used two methods to find some ξ such that $N_{\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}}(\xi) = b$.

The column '`NormEquation`' gives the time needed in seconds it took for that function to calculate a solution. It occurred occasionally that `NormEquation` was unable to calculate the class group and units, and `NormEquation` terminated with an error message. This we put down to too large a choice of a, and is marked in the table with `DNT`, standing for 'Did Not Terminate'.

The column 'Reduction' gives the time needed in seconds to run the reduction algorithm described by Algorithm 4.2.2, including the time needed to construct the actual solution. We make use of MAGMA's inbuilt reduction software. The solution generated by our method is usually very large, and therefore the various manipulations involved in constructing it are very costly in terms of memory. Unfortunately, we were not able to find a solution to this problem, and for our purposes the size of the final solution to the norm equation was immaterial.

a	b	`NormEquation`	Reduction
70235621210581	−27500445746285940545317086481911025746952636555 7	13.780	0.430
22679366817707	353154210985568215934586194305146764823031116 06	13.260	22.280
67587097421358	−14968473969767573656907418581217 1	DNT	0.090
−44425602641492	−12996440218868245919366463234813 61	19.140	0.090
85037766826631	38430740258311310904591339344963 14	21.170	0.380
2397945053545	46251657459282101408172703921 76	13.940	0.110
4350672676449	82436669472446904161048611975014 87	DNT	43.740
1587779723503	99087131077430168884026620000	DNT	9.010
−6071170898514	35877189226621322970938646462 56	20.790	0.560
−1135264462975	12888254007698352811051142 88	DNT	0.030
−3848271226757	−10971833750140538140987070369 70	DNT	0.090
1619769021285	63988240880515662976030972692	DNT	62.810
−9129186073582	27309519131866249767443222530 03	DNT	12.620

4.3 Modifications of the Theory of Reduction for K any Number Field

We now want to let the base field K be any number field with L some cubic extension of K. We will modify the methods discussed in Section 4.1 to solve norm equations of the form

$$N_{L/K}(\xi) = x.$$

If K is totally real, it still makes sense to speak of positive definite forms as in Definition 4.1.1. However, if K is imaginary, we need a new definition. Many references are available for the theory discussed in this section. We followed mostly [SC02, Cas71, EGM98].

Definition 4.3.1. The set of positive definite binary Hermitian forms, denoted by $H(\mathbb{C})$, are of the form

$$\begin{aligned} Q(X,Y) &= a|X|^2 + bX\overline{Y} + \overline{b}\overline{X}Y + c|Y|^2 \\ &= a(|X - tY| + u^2|Y|^2) \end{aligned}$$

with $a,c,u > 0$ and $b,t \in \mathbb{C}$.

The discriminant of such a form is given by

$$\Delta(Q) = 4(ac - |b|^2) \in \mathbb{R}_{>0}.$$

Also, the upper half plane is no longer sufficient to characterise these forms.

Definition 4.3.2. Upper hyperbolic space is defined as

$$\mathscr{H}_3 = \{(z,r) | z \in \mathbb{C}, r \in \mathbb{R}_{>0}\}.$$

We fix an embedding $O_K \hookrightarrow \mathbb{C}$. An action of $SL_2(O_K)$ on this upper half-space is given by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot (z,r) = \left(\frac{(\alpha z + \beta)(\overline{\gamma z} + \overline{\delta}) + \alpha\overline{\gamma} r^2}{|\gamma z + \delta|^2 + |\gamma|^2 r^2}, \frac{r}{|\gamma z + \delta|^2 + |\gamma|^2 r^2} \right).$$

To each positive definite binary Hermitian form Q in $H(\mathbb{C})$, we can thus associate a point $z(Q) = (t,u) \in \mathscr{H}_3$ with t,u such as given in Definition 4.3.1. There is an action of $SL_2(O_K)$ on $H(\mathbb{C})$, which corresponds to the action on $\mathscr{H}_3$, given by

$$Q(X,Y) \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = Q(\alpha X + \beta Y, \gamma X + \delta Y).$$

The discriminant of Q is invariant under this action. The action of $SL_2(O_K)$ on $\mathscr{H}_3$ is generated by

$$M_\times = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad\qquad M_\omega = \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}$$

where $\omega \in O_K$ and

$$M_\times(z,r) = \left(\frac{-\overline{z}}{|z|^2 + r^2}, \frac{r}{|z|^2 + r^2} \right) \qquad\qquad M_\omega(z,r) = (z + \omega, r).$$

The action is covariant on $z(Q)$ by which we mean that for each $g \in SL_2(O_K)$ we have

$$z(Q \cdot g) = g^{-1}(z(Q))$$

where the action of g is as given above. Each $SL_2(O_K)$ orbit in $\mathscr{H}_3$ then has a unique representative in some fundamental region $\mathscr{F}$. The calculation of such fundamental regions is a nontrivial task and is partially dealt with in [Mor13, Lin05, EGM98]. We only give two examples here.

Definition 4.3.3. Let $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$. Let

$$\begin{aligned} \mathscr{B}_K &= \left\{ (z,r) \in \mathscr{H}_3 \mid |cz + d|^2 + |d|^2 r^2 \geq 1 \text{ for all coprime } c,d \in O_K \right\} \\ F_{\mathbb{Q}(i)} &= \left\{ z \in \mathbb{C} \mid 0 \leq |\mathrm{Re}(z)| \leq \frac{1}{2},\ 0 \leq \mathrm{Im}(z) \leq \frac{1}{2} \right\} \\ F_{\mathbb{Q}(\sqrt{-3})} &= \left\{ z \in \mathbb{C} \mid 0 \leq \mathrm{Re}(z) \leq \frac{1}{2},\ -\frac{\sqrt{3}}{3}\mathrm{Re}(z) \leq \mathrm{Im}(z) \leq \frac{\sqrt{3}}{3}(1 - \mathrm{Re}(z)) \right\}. \end{aligned}$$

The *fundamental region* for K is then defined to be

$$\mathscr{F}_K = \{(z,r) \in \mathscr{B}_K \mid z \in F_K\}.$$

In this case, MAGMA does not have reduction software available yet, therefore we implemented the method ourselves. The method used to reduce a point $(z,r) \in \mathscr{H}_3$ to some point in the fundamental region is the following. If z is not within bounds, we act on (z,r) by some suitable M_ω. If z is within bounds but r is not, we act by $M_\times$. Thus we proceed until we have found the reduced point. This leads us naturally to the following definition.

Definition 4.3.4. We say a positive definite binary Hermitian form with coefficients lying in K is *reduced with respect to K* if the point associated to it lies in the proper fundamental domain.

Let

$$F(X,Y) = a_0X^3 + a_1X^2Y + a_2XY^2 + a_3Y^3$$

be a binary cubic with $a_i \in K$ and $a_0 \neq 0$. We also let $f(X) = F(X,1)$ as before. We follow [SC02], which cites various results by Julia [Jul17]. There are once again various ways of assigning a suitable point in either the upper half plane H or upper half space $\mathscr{H}_3$ to it.

If F is real with a single real root, Belabas [Bel97] uses the unique root in the upper half plane, whereas Cremona [Cre99] uses the point $t+ui$ where t and u are given by solving

$$\sum_{j=1}^{3} t_j(X-\alpha_jY)(X-\overline{\alpha}_jY) = (X-tY)^2 + u^2Y^2$$

where α_j are the roots of F and the t_j are carefully chosen.

For real cubics F with three real roots, we follow [Jul17] and associate to it the positive definite form

$$Q_0(F)(X,Y) = \sum_{j=1}^{3} \frac{1}{|f'(\alpha_j)|^2}(X-\alpha_jY)^2$$

The case we are most interested in however will be the case where F is a complex form. After all, we shall be most interested in adjoining a cube root of unity to $\mathbb{Q}$, hence $K = \mathbb{Q}(\sqrt{-3})$. For F a complex form, we define the positive definite Hermitian form

$$Q_0(F)(X,Y) = \sum_{j=1}^{3} \frac{|X-\alpha_jY|^2}{|f'(\alpha_j)|^2}. \tag{4.12}$$

Definition 4.3.5. Let F be a complex binary cubic with coefficients lying in K. Then we say F is *reduced with respect to K* if the associated positive definite binary Hermitian form $Q_0(F)$ given by (4.12) is reduced in the sense of Definition 4.3.4.

4.4 Improving the Norm Equation when K is a Number Field with Class Number 1

In this section, we discuss the changes that need to be made to Algorithm 4.2.2 to allow us to use it in a more general setting. First, we see that Theorem 4.2.1 holds over general number fields K. All we need to supply now is an analogue of the construction of the cubic (4.10), which we do for number fields K with class number 1.

Assume we have $a,b \in O_K$ such that b is a norm for the extension $K(\sqrt[3]{a})/K$. Without loss of generality, assume that $|N_{K/\mathbb{Q}}(a)| < |N_{K/\mathbb{Q}}(b)|$ and the ideal (b) is a cubefree product of prime ideals. Let $(b) =$

$(b_1)(b_2)^2$. Then, as was done in Section 4.2, we can now find $c \in O_K$ such that $a \equiv c^3 \bmod (b_1)$. We consider the binary cubic form

$$F(X,Y) = \frac{1}{b_1}\left((cX + b_1Y)^3 - aX^3\right) \in O_K[X,Y]. \tag{4.13}$$

This binary cubic can be reduced using the theory from the previous section. If we can find some $U,V \in O_K$ such that $F(X,Y)$ takes some small value, then we may observe that, as before

$$\begin{aligned} N_{K(\sqrt[3]{a})/K}(b_2\left((cU + b_1V) - \sqrt[3]{a}U\right)) &= b_1b_2^3F(U,V) \\ &\in (b)(b_2F(U,V)). \end{aligned}$$

What we would like to be true at this point is

$$|N_{K/\mathbb{Q}}(b_2F(U,V))| < |N_{K/\mathbb{Q}}(b)|$$

for then we would be able to define an iterative procedure as in Algorithm 4.2.2. Although it seems likely there exists some constant C_K such that we can find $U,V \in O_K$ with

$$|N_{K/\mathbb{Q}}(F(U,V))| \leq C_K\sqrt{|N_{K/\mathbb{Q}}(ab_1)|}$$

a true analogue to Theorem 4.1.4 is lacking. For number fields of small discriminant, we have had some success in employing this method, and we present some examples in the next section. In no case however do we avoid using MAGMA's `NormEquation` altogether. The best we were able to do is to reduce the sizes of a and b somewhat, thus giving an easier field to calculate class group and units over.

4.5 Examples

Example 4.5.1. Let $K = \mathbb{Q}(i)$, and take $a = 4423i + 18397$ and $b = -8611600044i + 4398890071$.

In the first step, we let $b = b_1b_2^2$ where

$$\begin{aligned} b_1 &= -8611600044i + 4398890071 \\ b_2 &= 1 \end{aligned}$$

First we form the cubic F from (4.13)

$$\begin{aligned} (&-84308437170258455335482453180209500871874269743 1i \\ &-43065579599016646537498059552142613078972385254 6)X^3 \\ &+131285795872884285167846565625958704742 7X^2Y \\ +(&5404472972471657953742759679 96i - 2760657993418700449533696765 39)XY^2 \\ &+(-75762963857949526248i - 54809421461078416895)Y^3 \end{aligned}$$

which we reduce to

$$\begin{aligned} &(496735i - 119333)X^3 + (-410556i - 251460)X^2Y \\ +&(283011i + 690831)XY^2 + (163053307i + 318733432)Y^3. \end{aligned}$$

In an attempt to find small solutions to this reduced cubic, we evaluate at the units of K and find that $(i,-i)$ gives a smaller solution than anything else we tried. This translates into the solution (U,V) on F given by

$$\begin{aligned} U &= 13289i + 55162 \\ V &= 119348489996606i + 28682661485346. \end{aligned}$$

Thus we have reduced the problem to

$$\begin{aligned} a &= 4423i + 18397 \\ b &= b_2 F(U,V) \\ &= -161863005i - 317910474. \end{aligned}$$

In the following tables, we show the iterations of the algorithm in this example. The first table gives the values of a and b at each step, as well as the operation carried out. The second table gives the values of c, U and V whenever relevant. Of course, if a step involves swapping a and b or any other manipulation not involving the cubic F, no such values need be given.

Iteration	a	b	Operation
1	$4423i+18397$	$-161863005i-317910474$	
2	$4423i+18397$	$-11077211i+8864955$	
3	$4423i+18397$	$100594i+641863$	
4	$4423i+18397$	$-107577i+105828$	
5	$4423i+18397$	$19133i-39085$	
6	$4423i+18397$	$-34534i+16836$	
7	$4423i+18397$	$-5565i-18477$	
8	$-1142i-80$	$-4781548804374i-4986421854330$	$a_{\text{new}}=a+b$, $b_{\text{new}}=a^2b$
9	$-1142i-80$	$-51218262489i+2441992664676$	
10	$-1142i-80$	$18454839i-124828522$	
11	$-1142i-80$	$38490i+70033$	
12	$-1142i-80$	$519i+1624$	
13	$-1142i-80$	$2216i-3246$	
14	$-1142i-80$	$278i+1370$	
15	$-1142i-80$	$273i-412$	
16	$-1142i-80$	$686i+92$	
17	$686i+92$	$-1142i-80$	$a_{\text{new}}=b$, $b_{\text{new}}=a$
18	$-456i+12$	$517656824i+181118368$	$a_{\text{new}}=a+b$, $b_{\text{new}}=a^2b$
19	$-456i+12$	$858641i-468288$	
20	$-456i+12$	$32148i-9984$	
21	$-456i+12$	$-10533i-5541$	
22	$-456i+12$	$-4910i-6984$	
23	$-456i+12$	$-3381i+4149$	
24	$-456i+12$	$-1628i-1162$	
25	$-456i+12$	$-1629i-939$	
26	$-456i+12$	$-332i-478$	
27	$-456i+12$	$-540i-188$	
28	$84i+200$	$114265152i+33155136$	$a_{\text{new}}=a-b$, $b_{\text{new}}=a^2b$
29	$84i+200$	$13941i+22563$	
30	$84i+200$	$-1422i+3594$	
31	$84i+200$	$1254i-543$	
32	$84i+200$	$-398i+86$	
33	$84i+200$	$121i+78$	
34	$84i+200$	$222i-74$	
35	$84i+200$	$-74i-37$	
36	$84i+200$	$-34i-10$	
37	$-34i-10$	$84i+200$	$a_{\text{new}}=b$, $b_{\text{new}}=a$
38	$-34i-10$	$29i-71$	
39	$-34i-10$	$100i-10$	
40	$-34i-10$	$-143i-23$	
41	$-34i-10$	$100i-10$	

Iteration	c	U	V
1	20919352752326754303	$13289i+55162$	$119348489996606i+28682661485346$
2	$-i-5394272038577216$	$3284i+1337$	$35078603365i+40546225814$
3	-73187635361206	$-93i-90$	$662237906i-84474409$
4	122477567466	$177i+68$	$30979925i+17830704$
5	$-i-2998327298$	$-66i-41$	$1500364i-363545$
6	-2633254	$4i+4$	$-5745i+926$
7	54485546	$-8i-30$	$16892i-86429$
10	$-i-1632680$	$30i+1$	$-1593i-3219$
11	$3i+260930819033420$	$-3696i+1866$	$6996223891i-4934858508$
13	-1432644	$-16i+9$	$15109i-3111$
14	1034489	$-8i-11$	$-2408i+6743$
16	-76276	$3i+4$	$727i+259$
20	1579	$2i+1$	$-25i-4$
22	-21718806	$52i+45$	$-28497i+122214$
23	-765972	$-12i+32$	$-3459i-5064$
24	3090684	$5i+6$	$4427i+862$
25	-443801	$-8i+13$	$-462i-6758$
26	-144066	$15i+5$	$242i+1187$
27	-44	-1	$2i$
30	-472	$2i+1$	$-4i-30$
32	50507	$-7i+14$	$-372i-443$
34	228	-1	$7i+3$
36	$11i-65$	$-3i+2$	$-2i-2$
39	1374	$-5i+4$	$56i-100$
40	$-i+195$	$i-5$	$-6i+19$
41	354	$6i-4$	$-12i-13$

At this point, when we carried on for three more iterations, we failed to improve the situation any further, thus we terminated here and used MAGMA's function `NormEquation`. Using `NormEquation` without any reductions takes 1.64 seconds. The final norm equation after 38 iterations took 0.31 seconds. However, in this particular case we were no better off. Due to issues with memory use, the entire procedure took 7.07 seconds. This was a consistent problem, because the solutions we generate are usually very large, in this case several pages long. Thus the overall gains are either not as great as in the $K=\mathbb{Q}$ case, or indeed nonexistent as in this example.

Example 4.5.2. Let $K=\mathbb{Q}(\zeta_3)$, and we seek ξ such that $N_{K(\sqrt[3]{a})/K}(\xi)=b$ where

$$\begin{aligned} a &= 5241592208466\zeta_3+9258597461771 \\ b &= -1871\zeta_3+2918. \end{aligned}$$

In the first step, we swap the roles of a and b. In the second step, we let $b=b_1b_2^2$ where

$$\begin{aligned} b_1 &= 5241592208466\zeta_3+9258597461771 \\ b_2 &= 1. \end{aligned}$$

The cubic F from (4.13) is given by

$$\begin{aligned}
&(-191048863341779851764326540897649444181225264214117234439472828 7\zeta_3\\
&+146414344565442321349430654875634320316863851979390190299234509 1)X^3\\
&+24661905259377214699307887711079436698347149136388 43X^2Y\\
&+(450855290339480696557943624444189030718\zeta_3+796377795285373177099824473254360886733)XY^2\\
&+(69585295754032436593033416\zeta_3+58247338079260924604383285)Y^3
\end{aligned}$$

which reduces to

$$\begin{aligned}
&(-14088991\zeta_3+177488443)X^3+(46530588\zeta_3-225776838)X^2Y\\
&+(169335189\zeta_3+110615553)XY^2+(-25046927\zeta_3+162160023)Y^3.
\end{aligned}$$

By considering the units of O_K, we find a small solution at $(-\zeta_3,-\zeta_3-1)$, giving the following small solution (U,V) on F.

$$\begin{aligned}
U &= 279323\zeta_3-518217\\
V &= -2350986297336096581\zeta_3+273823865257468289
\end{aligned}$$

Thus we have reduced the problem to

$$\begin{aligned}
a &= -1871\zeta_3+2918\\
b &= b_2F(U,V)\\
&= -172649809\zeta_3-120578644
\end{aligned}$$

The following table gives the values of a and b after each iteration, together with all unusual operations. The second table gives the values of c, U and V at all relevant steps. Once again, we stopped and used `NormEquation` when we failed to improve a and b for three steps.

Iteration	a	b	Operation
1	$-1871\zeta_3+2918$	$5241592208466\zeta_3+9258597461771$	
2	$-1871\zeta_3+2918$	$-172649809\zeta_3-12057864$	
3	$-1871\zeta_3+2918$	$-1982070\zeta_3-194831$	
4	$-1871\zeta_3+2918$	$-89847\zeta_3-22274$	
5	$-1871\zeta_3+2918$	$19238\zeta_3+541$	
6	$-1871\zeta_3+2918$	$786\zeta_3+3035$	
7	$786\zeta_3+3035$	$-1871\zeta_3+2918$	$a_{\text{new}}=b$, $b_{\text{new}}=a$
8	$2657\zeta_3+117$	$3811484077\zeta_3+32846307926$	$a_{\text{new}}=a-b$, $b_{\text{new}}=a^2b$
9	$2657\zeta_3+117$	$-1329574\zeta_3+10397075$	
10	$2657\zeta_3+117$	$145491\zeta_3+54274$	
11	$2657\zeta_3+117$	$29102\zeta_3+5279$	
12	$2657\zeta_3+117$	$31217\zeta_3+10562$	
13	$2657\zeta_3+117$	$9187\zeta_3+3627$	
14	$2657\zeta_3+117$	$2794\zeta_3+4953$	
15	$2657\zeta_3+117$	$121\zeta_3-212$	
16	$121\zeta_3-212$	$2657\zeta_3+117$	$a_{\text{new}}=b$, $b_{\text{new}}=a$
17	$121\zeta_3-212$	$1141\zeta_3+212$	
18	$121\zeta_3-212$	$227\zeta_3+576$	
19	$121\zeta_3-212$	$-33\zeta_3+275$	
20	$88\zeta_3+63$	$-21311059\zeta_3+6157140$	$a_{\text{new}}=a+b$, $b_{\text{new}}=a^2b$
21	$88\zeta_3+63$	$71696\zeta_3+54720$	
22	$88\zeta_3+63$	$8962\zeta_3+6840$	
23	$88\zeta_3+63$	$-355\zeta_3-192$	
24	$88\zeta_3+63$	$76\zeta_3+212$	
25	$88\zeta_3+63$	$132\zeta_3-72$	
26	$88\zeta_3+63$	$-76\zeta_3-212$	
27	$88\zeta_3+63$	$132\zeta_3-72$	
28	$88\zeta_3+63$	$-76\zeta_3-212$	

Iteration	c	U	V
2	2867164991147016563061534 1	$279323\zeta_3 - 518217$	$-2350986297336096581\zeta_3 + 273823865257468289$
3	6891413508236914	$2719\zeta_3 + 120$	$89955841994\zeta_3 + 135661075768$
4	804387530876	$238\zeta_3 - 181$	$91017146\zeta_3 + 178658486$
5	1182869459	$-46\zeta_3 + 47$	$-945129\zeta_3 - 1316429$
6	-170113893	$-12\zeta_3 - 46$	$415121\zeta_3 + 297336$
9	451445	$5\zeta_3 + 12$	$-957\zeta_3 - 1243$
10	-19497372065900	$231\zeta_3 + 680$	$521099256\zeta_3 + 1208548845$
11	5944729415	$-110\zeta_3 - 35$	$321837\zeta_3 + 4696354$
12	304916947	$59\zeta_3 - 1$	$-143994\zeta_3 - 736048$
13	7115800	$6\zeta_3 - 12$	$-20391\zeta_3 + 12494$
14	21272	$2\zeta_3 - 3$	$-464\zeta_3 - 84$
15	$-30\zeta_3 - 17749$	$17\zeta_3 + 7$	$62\zeta_3 + 60$
17	-1444031	$24\zeta_3 + 10$	$-5074\zeta_3 + 8193$
18	29	ζ_3	$-4\zeta_3 - 3$
19	110963	$-2\zeta_3 + 4$	$905\zeta_3 - 414$
21	3775	$3\zeta_3 + 8$	$-56\zeta_3 + 48$
23	-8069499	$-30\zeta_3 - 43$	$22094\zeta_3 - 21781$
24	38383	$3\zeta_3 + 10$	$-1205\zeta_3 - 229$
25	-167	$-3\zeta_3$	$-12\zeta_3 - 4$
26	-82	$-\zeta_3 - 2$	$9\zeta_3 - 2$
27	-167	$3\zeta_3$	$-12\zeta_3 - 4$
28	-82	$-\zeta_3 - 2$	$9\zeta_3 - 2$

In this case, this method took 9.67 seconds whereas MAGMA's function `NormEquation` failed to terminate at all and gave an error message. However, most of the gain was made in the first step, where the roles of a and b are swapped. If we do just this one step, then `NormEquation` will find a solution in 2.34 seconds.

Once again, we give tables as an indication of the efficacy of our method, which once again should be seen as simply a beginning point of a comparison between our method and `NormEquation`. Version 2.21-1 of MAGMA was used. We generated a and b as follows. We randomly generated an element of O_K, which became a. We then randomly generated three more elements $b_0, b_1, b_2 \in O_K$ and let $b = N_{K(\sqrt[3]{a})/K}(b_0 + b_1\sqrt[3]{a} + b_2\sqrt[3]{a}^2)$. We always ensured that $|a| < |b|$, swapping their roles if necessary to achieve this, and as before used two methods to find some ξ such that $N_{K(\sqrt[3]{a})/K}(\xi) = b$.

Once again, the column '`NormEquation`' simply gives the time in seconds it took that function to calculate a solution. Whenever `DNT` occurs in the table, we mean 'Did Not Terminate', indicating that `NormEquation` terminated with an error message, having failed to compute class group and units.

The column 'Reduction' is slightly different to before. It includes, as before, the time needed in seconds to run the reduction algorithm described by Algorithm 4.2.2. The reduction algorithm is terminated when no improvement is noted for 5 steps. It also includes the time taken by `NormEquation` whenever it was called after the reduction steps have been completed. It does not include the time needed to construct the actual solution. The solutions generated by our method are even larger than before, and therefore usually extremely costly in terms of memory in examples of this size. Once again, we did not improve the situation, as in our case the size of the final solution was of no real consequence. However, for large a and b, such as in all these examples, the solution becomes large enough that performing the manipulations necessary to obtain it becomes the major bottleneck in using this method.

a	b	NormEquation	Reduction
$-27562318i+33109835$	$-103284999619841438i-79089466538861573$	62.350	19.310
$-46712519i-464220447$	$-27472198206344200772i+20024220036079386021$	2255.320	1373.690
$457960311i-234115155$	$-44006495293562970851i-28529403607371780864$	781.370	419.890
$-124707062i+391128728$	$10783543850541390003i-10532976641434724246$	1080.560	35.090
$-126198355i+220425997$	$-261292726606350282i-445078391789136785$	49.130	14.840
$-8432287i+384179478$	$57329560246058685 47i+17545240966260470045$	76.140	186.730
$276885337i-471639922$	$55641755391090371 12i+36972365783474880430$	1494.190	251.750
$489000712i-328198170$	$43336395324184322968i+1251651780103417755$	48.790	41.450
$-91576685i+304856091$	$-5411260473399890435i-3573466872151010722$	71.090	19.650
$193891176i+254082924$	$-12316109224473215768i-3370543074315767792$	DNT	29.470
$191906135i+427234837$	$-272091453194804879 71i+33924655077631708013$	DNT	29.470
$325301729i-473884263$	$-360616950612912220 86i+36901999513041951040$	DNT	42.330
$-216199489i-387453958$	$-472374034813894139 1i+24150206431716762912$	DNT	190.860
$-188114304i+111202938$	$-2677614557268003992i-1473337482898372474$	768.830	44.890
$268911775i-261940316$	$66316126656260750 37i-16319851779660481657$	DNT	41.660
$-20190685i+233949106$	$-604619955768772962i+3476769170641517807$	DNT	33.090
$193785866i+224652580$	$74935306473451553 38i-11524268297440878643$	1617.630	23.410
$26159881i+402165884$	$18136660970237766 93i+90652646356328149$	897.720	1021.660
$-164038284i+469514217$	$16651782553041717212i-14566497988710989061$	1507.000	30.890
$-370873557i+41897030$	$-417172086757742807 80i-26178708265157879292$	1609.080	1889.230
$-301779187i+48627567$	$-492415549255337811 9i-17857291052882736816$	705.200	117.260
$-201495298i-419599470$	$18160890962090754 00i+16446131941587141800$	DNT	754.500

$$K = \mathbb{Q}(i)$$

a	b	NormEquation	Reduction
$-13117310\zeta_3+20485456$	$-45407490549174094\zeta_3+15845760531070777$	37.640	26.130
$19500539\zeta_3+67414560$	$-1002726158222333548\zeta_3-639625061508336295$	37.840	92.320
$17654008\zeta_3+44894405$	$51221253198625798\zeta_3-20234237483800700$	75.260	22.230
$42069760\zeta_3+48169862$	$-117125700432341148\zeta_3-196123187948007310$	166.950	35.150
$44619028\zeta_3+57662742$	$66439618595133870\zeta_3-186544994879554753$	53.450	58.710
$-8763389\zeta_3-11562734$	$-1150055925466495\zeta_3+1184392823592454$	22.340	24.870
$25641944\zeta_3+5452118$	$329123967637738432\zeta_3-48008738885204225$	49.830	24.580
$-42350469\zeta_3-87197764$	$144662538899383071\zeta_3-128986869988808313$	58.070	22.350
$-119396194\zeta_3-43331483$	$-2841730297308096884\zeta_3-1255515734638964560$	192.550	146.550
$-48224998\zeta_3+139576914$	$-608778188585304958\zeta_3-267025105708703262$	98.510	44.830
$100433947\zeta_3+302923891$	$337773378670492680\zeta_3-59536460350213867$	168.420	139.510
$-431103241\zeta_3-678475775$	$-408301311705359452 32\zeta_3+50901557742038349221$	903.690	78.490
$422360594\zeta_3+356187537$	$-3155890525775461988\zeta_3+13068040367707186229$	72.430	63.330
$-241818089\zeta_3-472672811$	$-2425748903399313279\zeta_3+12507270312698920511$	605.710	47.570
$-431103241\zeta_3-678475775$	$-408301311705359452 32\zeta_3+50901557742038349221$	903.690	78.490
$422360594\zeta_3+356187537$	$-3155890525775461988\zeta_3+13068040367707186229$	72.430	63.330
$-241818089\zeta_3-472672811$	$-2425748903399313279\zeta_3+12507270312698920511$	605.710	47.570
$-248408455\zeta_3-213297663$	$-3541050136385600 43\zeta_3+129686925086796494$	437.910	36.160
$489868457\zeta_3+951252259$	$-5536046801249419258\zeta_3-5319278065273988657$	1497.720	574.860
$-469622158\zeta_3-668672343$	$-8765517188520885368\zeta_3+112977738595208318858$	2003.690	1430.610
$-384730604\zeta_3-767444897$	$-11947538914288076931\zeta_3-11905758861046548528$	1458.050	414.600
$-27562318\zeta_3+33109835$	$-1032849996198414 38\zeta_3-79089466538861573$	DNT	25.050

$$K=\mathbb{Q}(\zeta_3)$$

Chapter 5

Methods for Computing the Pairing in the Three Isogeny Case

In this chapter, we compute the Cassels-Tate pairing using the two definitions given in Chapter 3. We call the two methods the direct Weil pairing method and the pushout form method. We give several examples of the method in action in each case.

5.1 Direct Weil Pairing Method

Let E/K be an elliptic curve admitting a 3-isogeny $\phi : E \to \hat{E}$. Let $E[3] = \langle S, T \rangle$ such that $\ker(\phi) = \langle S \rangle$. In this section, we will use the Weil pairing definition of the Cassels-Tate pairing, given in Definition 3.1.6, to calculate the pairing on $S^{(\hat{\phi})}(\hat{E}/K) \times S^{(\hat{\phi})}(\hat{E}/K)$. We first outline the procedure, and then move on to some examples of this method.

We saw in Definition 3.1.6 that the Cassels-Tate pairing is given by the sum of a number of local pairings. By a slight variation of Proposition 3.3.6, these primes are given by the set of bad primes of E, together with possibly the primes involved in the global lift choice.

Suppose that we are in one of the three cases outlined in Section 2.5, and suppose that $x, y \in S^{(\hat{\phi})}(\hat{E}/K)$. Let v be some place at which we want to calculate the local pairing. Let R be the étale algebra corresponding to the set $E[3] \setminus \{\mathscr{O}\}$. We saw in Section 2.5 that in the three cases we are considering, we always have $R \cong L_1 \times L_2$ for some finite separable field extensions L_1 and L_2 corresponding to the orbits of S and T, respectively. We write R_v, $L_{1,v}$ and $L_{2,v}$ for the localisations at v. Then the local pairing is calculated as follows.

Procedure 5.1.1. *This procedure calculates the local pairing between $x, y \in S^{(\hat{\phi})}(\hat{E}/K)$ at some place v of K, in the cases that $\phi : E \to \hat{E}$ is of types μ_3-nonsplit, $\mathbb{Z}/3\mathbb{Z}$-nonsplit or generic 3-isogeny.*

1. *Lift $x \in H^1(K, \hat{E}[\hat{\phi}])$ to $x_1 \in H^1(K, E[3])$, which is possible by Lemma 3.1.10. Explicitly, we can use one of Lemmas 2.5.9, 2.5.12 or 2.5.15. We then obtain x_1 as an element $(a,b) \in R^\times/(R^\times)^3$.*
2. *Let $(a_v, b_v) = (x_1)_v \in R_v^\times/(R_v^\times)^3$ be the element obtained by localising the coordinates of x_1 at v.*
3. *From Corollary 3.4.9 we have a map*

$$h : E(K) \longrightarrow R^\times/(R^\times)^3$$

given by the tangent lines at S and T. We also have the local version for every place v of K

$$h_v : E(K_v) \longrightarrow R_v^\times/(R_v^\times)^3.$$

4. *For this step, see exact complex* (3.8)*. We find some local point $P_v \in E(K_v)$ such that $h_v(P_v) = (r_v,t_v) \in R_v^\times/(R_v^\times)^3$ and $r_v \equiv a_v \bmod (L_{1,v}^\times)^3$. We have that $\phi(r_v,t_v) = \phi(a_v,b_v)$, thus they differ by some element in the image of $\iota_{\phi,v}$. In fact, they differ by $\xi_v = \frac{b_v}{t_v}$.*

5. *Let y_v be the localisation of $y \in H^1(K,\hat{E}[\hat{\phi}])$ to $y_v \in H^1(K_v,\hat{E}[\hat{\phi}])$.*

6. *We now have the 2 elements required in Definition 3.1.6 and calculate the local Tate pairing $< \xi_v, y_v >_{v,e_\phi}$ from Definition 3.1.4.*

We now illustrate this procedure with two examples.

Example 5.1.2. Let E be the curve 63531c1 from the Cremona database [Cre15].

$$E : y^2 = x^3 - 3(4x+52)^2$$

We are in the μ_3-nonsplit case. The isogenous curve is $\hat{E} : y^2 = x^3 + 36^2(x+543)^2$. The points of order 3 on E are generated by $S = (0, 52\sqrt{-3})$ and $T = (\beta, 4(\beta+39))$ where β is a root of $\gamma(x) = x^3 - 64x^2 - 2496x - 32448$. We also choose a cube root of unity $\zeta_3 = -\frac{1}{2} - \frac{\sqrt{-3}}{2}$.

The various number fields involved are given by $L_1 = \mathbb{Q}(\zeta_3)$, $L_2 = \mathbb{Q}(\sqrt[3]{181})$ and $M = \mathbb{Q}(\zeta_3, \sqrt[3]{181})$. The Selmer groups are given by the following generators

$$S^{(\phi)}(E/\mathbb{Q}) = \langle 181 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^3$$
$$S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) = \langle \zeta_3, -39\zeta_3 - 52 \rangle \subset \left(L_1^\times/(L_1^\times)^3\right)^-.$$

The initial estimate for the rank of E is therefore 2 by Section 2.7. The discriminant of E is $-43977682944 = -2^{12} \cdot 3^3 \cdot 13^3 \cdot 181$, therefore the initial set of primes S for which we must do a local pairing calculation is given by

$$P = \{2, 3, 13, 181, \infty\}.$$

This set may need to be enlarged depending on the global lifts made, however this does not happen in this example.

From Exercise 2.7 of [CF67], we see that we can ignore the infinite place, as 3 is odd. We now follow Procedure 5.1.1 to calculate the Cassels-Tate pairing on $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) \times S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$.

In step 1, we first lift ζ_3 and $-39\zeta_3 - 52$ globally to $H^1(\mathbb{Q}, E[3]) = H$, where $H \subset L_1^\times/(L_1^\times)^3 \times L_2^\times/(L_2^\times)^3$ is given by Lemma 2.5.7 and the lift to it is given by Lemma 2.5.9. Note that this lift need only be correct up to cubes.

	global lifts in H
ζ_3	$(\zeta_3, \frac{1}{3}(28\sqrt[3]{181}^2 + 160\sqrt[3]{181} + 868))$
$-39\zeta_3 - 52$	$(-39\zeta_3 - 52, \frac{1}{3}(59\sqrt[3]{181}^2 + 314\sqrt[3]{181} + 3011))$

In step 2, we localise these global lifts at each $p \in P$. The following table gives the element b_p in each case. Note that 181 is a cube in $\mathbb{Q}_p$ for all $p \in P \setminus \{\infty\}$ except $p = 181$.

	$b_2 \bmod 2^9$	$b_3 \bmod 3^{10}$	$b_{13} \bmod 13^3$	$b_{181} \bmod 181^3$
ζ_3	256	25366	1710	$3953170\sqrt[3]{181}^2 + 3953214\sqrt[3]{181} + 3953450$
$-39\zeta_3 - 52$	312	39366	1352	$1976600\sqrt[3]{181}^2 + 1976685\sqrt[3]{181} + 1977584$

Step 3 is to give the map $h : E(\mathbb{Q}) \to L_1^\times/(L_1^\times)^3 \times L_2^\times/(L_2^\times)^3$ explicitly. It is given by the tangent lines at S and T, thus $h = (\tan_S, \tan_T)$, where

$$\tan_S(x,y) = y - 4\sqrt{-3}x - 52\sqrt{-3}$$
$$\tan_T(x,y) = y - \frac{3\beta^2 - 96\beta - 1248}{8(\beta+39)}x + 8\beta + 156.$$

In step 4, we find local points on E that satisfy certain properties. The following table gives the local points we found.

	mod 2^9	mod 3^{10}	mod 13^3	mod 181^3
ζ_3	$(4:4:3)$	$(27:108:108)$	$(6:107:1)$	$(1:5483060:1)$
$-39\zeta_3 - 52$	$(4:4:3)$	$(3:143:2700)$	$(13:117:1)$	$(1:5483060:1)$

We thus find the following elements ξ_p, modulo cubes.

	$\xi_2 \bmod 2^3$	$\xi_3 \bmod 3^5$	$\xi_{13} \bmod 13^3$	$\xi_{181} \bmod 181^3$
ζ_3	4	45	263	1
$-39\zeta_3 - 52$	7	189	169	1

In step 5 we specify a localisation for each generator of the Selmer group.

	$y_2 \bmod 2^3$	$y_3 \bmod 3^3$	$y_{13} \bmod 13^3$	$y_{181} \bmod 181^3$
ζ_3	$6+6\sqrt{-3}$	$13+13\sqrt{-3}$	1036	3177503
$-39\zeta_3 - 52$	$4+4\sqrt{-3}$	$8+6\sqrt{-3}$	1287	601892

In step 6, we use Section 3.2 to compute the local pairings in each case. The prime 2 is inert in L_1, but the situation is different for the primes 13 and 181, which both split into two distinct places. Thus in the final sum, we must multiply the result obtained from these primes by two, as stated in Remark 3.2.4. The following table gives the necessary information to calculate the local pairing at 2.

$(\xi_2, y_2)_2$	$\mathrm{val}_2(\xi)$	$\mathrm{val}_2(y)$	c	$\left(\frac{c}{2}\right)$
$(4, 6+6\sqrt{-3})_2$	2	2	$\frac{1}{18}(-1-\sqrt{-3})$	1
$(7, 6+6\sqrt{-3})_2$	0	2	49	0
$(4, 4+4\sqrt{-3})_2$	2	3	$\frac{1}{2}(-1-\sqrt{-3})$	1
$(7, 4+4\sqrt{-3})_2$	0	3	343	0

Thus the local pairing at 2 is given by the following matrix.

	ζ_3	$-39\zeta_3 - 52$
ζ_3	1	1
$-39\zeta_3 - 52$	0	0

We choose the prime $p_{13} = 1 - 3\zeta_3$ lying over 13 and $p_{181} = -4\zeta_3 - 15$ lying over 181. The following tables give the information needed to compute the local pairings at these primes, as well as the matrix for the result of the local pairing. Denote by η_g the element obtained from the Selmer element g for prime 181.

$(\xi_{13}, y_{13})_{p_{13}}$	$\mathrm{val}_{p_{13}}(\xi)$	$\mathrm{val}_{p_{13}}(y)$	c	$\left(\frac{c}{p_{13}}\right)$
$(263, 1036)_{p_{13}}$	0	0	1	0
$(169, 1036)_{p_{13}}$	2	0	$\frac{1}{1073296}$	2
$(263, 1287)_{p_{13}}$	0	1	263	1
$(169, 1287)_{p_{13}}$	2	1	$\frac{1}{9801}$	0

	ζ_3	$-39\zeta_3 - 52$
ζ_3	0	2
$-39\zeta_3 - 52$	1	0

$(\xi_{181}, y_{181})_{p_{181}}$	$\mathrm{val}_{p_{181}}(\xi)$	$\mathrm{val}_{p_{181}}(y)$	c	$\left(\frac{c}{2}\right)$
$(1, 3177503)_{p_{181}}$	0	0	1	0
$(1, 601892)_{p_{181}}$	0	0	1	0

	ζ_3	$-39\zeta_3 - 52$
ζ_3	0	0
$-39\zeta_3 - 52$	0	0

To compute the local pairing at the prime 3, we need to use Proposition 3.2.7. Each element lies in a class generated by $\langle \lambda, \eta_1, \eta_2, \eta_3 \rangle$. The following table shows which class it is.

element	class	element	class
45	$\lambda\eta_1\eta_2\eta_3$	$13 + 13\sqrt{-3}$	η_1
189	$\eta_2^2\eta_3^2$	$8 + 6\sqrt{-3}$	η_3^2

Using Table 3.1, we find the following for the local pairing at 3.

	ζ_3	$-39\zeta_3 - 52$
ζ_3	2	1
$-39\zeta_3 - 52$	1	0

When we add the matrices obtained from the pairings at 2, 3 and 13, we obtain the following matrix for the Cassels-Tate pairing.

	ζ_3	$-39\zeta_3 - 52$
ζ_3	0	1
$-39\zeta_3 - 52$	2	0

Thus we see that the rank of E must be 0 and we have found

$$Ш(\hat{E}/\mathbb{Q})[\hat{\phi}] \cong (\mathbb{Z}/3\mathbb{Z})^2.$$

Example 5.1.3. Let E be curve 24060f1 in the Cremona database, given by

$$E : y^2 = x^3 + (x+15)^2.$$

We are in the $\mathbb{Z}/3\mathbb{Z}$-nonsplit case. The isogenous curve is $\hat{E} : y^2 = x^3 - 3\left(x + \frac{401}{9}\right)^2$. The points of order 3 on E are generated by $S = (0,15)$ and $T = (\beta, \frac{1}{3}(-2\zeta - 1)\beta - 30\zeta - 15)$ where β is a zero of $f(x) = x^3 + \frac{4}{3}x^2 + 60x + 900$. We have $L_1 = \mathbb{Q}(\zeta_3)$, $L_2 = \mathbb{Q}(\sqrt[3]{802})$ and $M = \mathbb{Q}(\zeta_3, \sqrt[3]{802})$. The Selmer groups are

$$S^{(\phi)}(E/\mathbb{Q}) = \langle 1 \rangle \subset L_1^\times/(L_1^\times)^3$$
$$S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) = \langle 2,3,5 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^3.$$

Thus we estimate the rank to be at most 2. The discriminant of E is -21654000, thus the set of primes for which we must do the local pairing calculation is given by

$$P = \{2,3,5,401\}.$$

Once again, we choose global lifts such that this set is not enlarged. We follow Procedure 5.1.1 to calculate the Cassels-Tate pairing. For step 1, we use Lemma 2.5.12 to lift the generators of $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ to $H^1(\mathbb{Q}, E[3])$. These global lifts are given in the following table.

	global lifts
2	$\frac{1}{3}(5\zeta_3+5)\sqrt[3]{802}^2 + \frac{1}{3}(15\zeta_3+4)\sqrt[3]{802} + \frac{1}{3}(-41\zeta_3+249)$
3	$\frac{5}{3}\sqrt[3]{802}^2 - \frac{7}{3}\zeta_3\sqrt[3]{802} + \frac{1}{3}(490\zeta_3+277)$
5	$\frac{1}{3}(34\zeta_3+7)\sqrt[3]{802}^2 + \frac{1}{3}(-251\zeta_3-317)\sqrt[3]{802} + \frac{1}{3}(-308\zeta_3+2683)$

In step 2, we localise the element obtained at each prime $p \in P$.

	$b_2 \bmod 2^3$	$b_3 \bmod 3^3$	$b_5 \bmod 5^3$	$b_{181} \bmod 401^3$
2	$(5\zeta_3+5)\sqrt[3]{802}^2 + (7\zeta_3+4)\sqrt[3]{802} + 7\zeta_3 + 1$	$-8\zeta_3 + 213$	$58\zeta_3 + 77$	$(45\zeta_3+45)\sqrt[3]{802}^2 + (135\zeta_3+36)\sqrt[3]{802} - 369\zeta_3 + 2241$
3	$5\sqrt[3]{802}^2 + \zeta_3\sqrt[3]{802} + 2\zeta_3 + 5$	$-206\zeta_3 + 36$	$23\zeta_3 + 24$	$45\sqrt[3]{802}^2 - 63\zeta_3\sqrt[3]{802} + 4410\zeta_3 + 2493$
5	$(2\zeta_3+7)\sqrt[3]{802}^2 + (5\zeta_3+3)\sqrt[3]{802} + 4\zeta_3 + 3$	$-214\zeta_3 + 35$	$48\zeta_3 + 78$	$(306\zeta_3+63)\sqrt[3]{802}^2 + (-2259\zeta_3-2853)\sqrt[3]{802} - 2772\zeta_3 + 24147$

In step 3, we find the map $h : E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^3 \times M^\times/(M^\times)^3$. It is given by $h = (\tan_S, \tan_T)$, where

$$\tan_S(x,y) = y - x - 15$$
$$\tan_T(x,y) = y - \left(\frac{1}{30}(2\zeta+1)\beta^2 + \frac{1}{45}(4\zeta+2)\beta + 2\zeta + 1\right)x - \left(\frac{1}{3}(4\zeta+2)\beta + 30\zeta + 15\right).$$

In step 4, we find a suitable local point on E for each generator and prime $p \in P$. The ones we chose are given in the following table.

	mod 2^3	mod 3^3	mod 5^3	mod 401^3
2	$(2:3:1)$	$(-2:12:-10)$	$(-4:3:-8)$	$(0:1:47286214)$
3	$(1:3:1)$	$(-3:9:6)$	$(-3:20:-7)$	$(0:3:0)$
5	$(1:5:1)$	$(-5:3:2)$	$(-5:15:1)$	$(0:5:0)$

These yield the following elements ξ_v which we will use in the pairing.

	$\xi_2 \bmod 2^3$	$\xi_3 \bmod 3^5$	$\xi_5 \bmod 5^3$	$\xi_{401} \bmod 401^3$
2	ζ_3	$-388\zeta_3 - 87$	$119\zeta_3 + 76$	ζ_3
3	1	$-244\zeta_3 + 36$	$6\zeta_3 + 98$	1
5	1	$-50\zeta_3 + 52$	$93\zeta_3 + 73$	1

In step 5, we find the following localisations of the Selmer group generators, which in this case we need not write out.

In step 6, we compute the local pairings, using Section 3.2. The prime 2 is inert in L_1, and the following table gives the necessary information to calculate the local pairing at 2.

$(\xi_2, y_2)_2$	$\mathrm{val}_2(\xi)$	$\mathrm{val}_2(y)$	c	$\left(\frac{c}{2}\right)$
$(\zeta_3, 2)_2$	0	1	ζ	1
$(\zeta_3, 3)_2$	0	0	1	0
$(\zeta_3, 5)_2$	0	0	1	0
$(1, 2)_2$	1	0	1	0
$(1, 3)_2$	0	0	1	0
$(1, 5)_2$	0	0	1	0

We therefore obtain the following for the local pairing at 2.

	2	3	5
2	1	0	0
3	0	0	0
5	0	0	0

The primes 5 and 401 are both inert as well. The following tables and matrices give the local pairing at these primes.

$(\xi_5, y_5)_5$	$\mathrm{val}_5(\xi)$	$\mathrm{val}_5(y)$	c	$\left(\frac{c}{2}\right)$
$(119\zeta_3 + 76, 2)_5$	0	0	1	0
$(119\zeta_3 + 76, 3)_5$	0	0	1	0
$(119\zeta_3 + 76, 5)_5$	0	1	$119\zeta_3 + 76$	1
$(6\zeta_3 + 98, 2)_5$	0	0	1	0
$(6\zeta_3 + 98, 3)_5$	0	0	1	0
$(6\zeta_3 + 98, 5)_5$	0	1	$6\zeta_3 + 98$	0
$(93\zeta_3 + 73, 2)_5$	0	0	1	0
$(93\zeta_3 + 73, 3)_5$	0	0	1	0
$(93\zeta_3 + 73, 5)_5$	0	1	$93\zeta_3 + 73$	1

	2	3	5
2	0	0	1
3	0	0	0
5	0	0	1

$(\xi_{401}, y_{401})_{401}$	$\mathrm{val}_{401}(\xi)$	$\mathrm{val}_{401}(y)$	c	$\left(\frac{c}{2}\right)$
$(2, \zeta_3)_{401}$	0	0	1	0
$(3, \zeta_3)_{401}$	0	0	1	0
$(5, \zeta_3)_{401}$	0	0	1	0
$(2, 1)_{401}$	0	0	1	0
$(3, 1)_{401}$	0	0	1	0
$(5, 1)_{401}$	0	0	1	0

	2	3	5
2	0	0	0
3	0	0	0
5	0	0	0

To compute the local pairing at the prime 3, we need to use Proposition 3.2.7. Each element lies in a class generated by $\langle \lambda, \eta_1, \eta_2, \eta_3 \rangle$. The following table shows which class it is.

element	class	element	class
$-388\zeta_3-87$	$\eta_1\eta_2^2\eta_3$	2	$\eta_2^2\eta_3^2$
$-244\zeta_3+36$	η_1	3	$\lambda^2\eta_1^2$
$-50\zeta_3+52$	$\eta_1^2\eta_3$	5	$\eta_2\eta_3$

Using Table 3.1, we find the following for the local pairing at 3.

	2	3	5
2	2	1	1
3	2	0	1
5	1	2	2

Adding together all our local pairings, we obtain the following matrix for the Cassels-Tate pairing.

	2	3	5
2	0	1	2
3	2	0	1
5	1	2	0

Thus we see that we must have $\text{rank}(E)=0$ again and

$$Ш(\hat{E}/\mathbb{Q}) = (\mathbb{Z}/3\mathbb{Z})^2.$$

The matrix we calculated is skew-symmetric as required, suggesting that the calculation is correct. There is a further check we can do, for the kernel of the pairing must be the image of $E(\mathbb{Q})/\hat{\phi}(\hat{E}(\mathbb{Q}))$. In this case, we have $E(\mathbb{Q})/\hat{\phi}(\hat{E}(\mathbb{Q})) = \langle S\rangle$. The torsion points S, $-S$ correspond to the Selmer elements 30^2 and 30 respectively, both of which are in the kernel, as required.

5.2 Examples of the Pushout Form Method

In this section we compute the Cassels-Tate pairing using the definition given in Definition 3.3.2. In Section 3.5, there is a calculation showing how to explicitly derive the pushout form from the discussion presented in Section 3.4. The author has a program to compute the Cassels-Tate pairing in 3 cases: μ_3-nonsplit, $\mathbb{Z}/3\mathbb{Z}$-nonsplit and generic 3-isogeny.

Example 5.2.1. We once again take $E: y^2 = x^3 - 3(4x+52)^2$, the same as in Example 5.1.2. The relevant Selmer group is

$$S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) = \langle \zeta_3, -39\zeta_3 - 52\rangle.$$

In this example, we shall compute the pairing on the whole of the Selmer group rather than just the generators. This is so that we can provide many examples of covering curves and pushout forms, and thereby illustrate fully the pushout form method. We shall also check the final result thoroughly to give confidence that the computations are correct and the code we used does the right work.

Using the calculation in Section 3.4, we compute the equations for the covering curves and pushout forms. Although these curves work in the calculations, the pushout forms were not in a simple form and had extremely large coefficients. They have therefore been simplified as was described in Section 3.6. For f a pushout form with $\text{div}(f) = 3\cdot A$, we found some f' with $\text{div}(f') = 3\cdot A'$ where A' is linearly equivalent to A. The covering curves are calculated using (2.15) and are given by the following table.

Selmer group element	covering curve
1	$-3x^2y+4x^2z+3xy^2-4xyz+4y^2z+13z^3=0$
ζ_3	$-x^3+4x^2z+3xy^2-4xyz-y^3+4y^2z+13z^3=0$
ζ_3+1	$-x^3+3x^2y+4x^2z-4xyz-y^3+4y^2z+13z^3=0$
$-39\zeta_3-52$	$x^3+4xy^2-4xyz+4xz^2+3y^3-12y^2z+3yz^2+3z^3=0$
$2535\zeta_3+1183$	$x^3+4xy^2-4xyz+4xz^2-3y^3-3y^2z+12yz^2-3z^3=0$
$-52\zeta_3-13$	$x^3+4xy^2-4xyz+4xz^2+4y^3-3y^2z-9yz^2+4z^3=0$
$-13\zeta_3+39$	$x^3+4xy^2-4xyz+4xz^2+y^3+9y^2z-12yz^2+z^3=0$
$1183\zeta_3-1352$	$x^3+4xy^2+4xyz+4xz^2+y^3-9y^2z-12yz^2-z^3=0$
$-1352\zeta_3-2535$	$x^3+4xy^2+4xyz+4xz^2-4y^3-3y^2z+9yz^2+4z^3=0$

The pushout forms are calculated using Section 3.5.3 and are given by the following table.

Selmer group element	pushout form
1	$6912x^2y-9216x^2z+6912xy^2-27648xyz+24576xz^2+9216y^2z$ $-49152yz^2+2816z^3$
ζ_3	$54x^3+51x^2y-410x^2z-405xy^2-58xyz+223xz^2+239y^3+361y^2z$ $+601yz^2+110z^3$
ζ_3+1	$746x^3-1398x^2y+474x^2z+555xy^2-843xyz+2223xz^2+53y^3$ $-381y^2z-540yz^2+93z^3$
$-39\zeta_3-52$	$601x^3+2262x^2y-1527x^2z+6885xy^2-2124xyz-3204xz^2+7884y^3$ $+2835y^2z-3456yz^2-999z^3$
$2535\zeta_3+1183$	$686x^3+2514x^2y+4809x^2z+4465xy^2+3401xyz-3248xz^2+9240y^3$ $+11049y^2z+5727yz^2-75z^3$
$-52\zeta_3-13$	$-20x^3+111x^2y+354x^2z-214xy^2-101xyz+524xz^2+485y^3$ $+651y^2z+297yz^2+260z^3$
$-13\zeta_3+39$	$74x^3+80x^2y-1294x^2z+199xy^2+1451xyz-1223xz^2-278y^3$ $-1551y^2z-2109yz^2-1300z^3$
$1183\zeta_3-1352$	$164x^3+351x^2y+261x^2z-355xy^2-1228xyz+572xz^2-161y^3$ $+1731y^2z-1629yz^2-154z^3$
$-1352\zeta_3-2535$	$279x^3+196x^2y+644x^2z-852xy^2+72xyz+2088xz^2+379y^3$ $-579y^2z-1674yz^2+2344z^3$

The set of bad primes of E is $P=\{3,13,181\}$, which in this case we need not enlarge (see Proposition 3.3.6). The Cassels-Tate pairing is given by the sum of local pairings, which can be calculated using Section 3.2. Definition 3.3.2 calls for finding a local point on our covering curves for each $p\in P$, and the ones we found are given in the following table.

Selmer group element	mod 3^5	mod 13^3	mod 181^3
1	$(1:0:0)$	$(1:0:0)$	$(1:0:0)$
ζ_3	$(8:0:1)$	$(1811:0:1)$	$(570452:0:1)$
ζ_3+1	$(8:0:1)$	$(1811:0:1)$	$(570452:0:1)$
$-39\zeta_3-52$	$(6:1:0)$	$(1974:0:1)$	$(531613:0:1)$
$2535\zeta_3+1183$	$(237:1:0)$	$(223:0:1)$	$(5429561:0:1)$
$-52\zeta_3-13$	$(208:0:1)$	$(679:3:1)$	$(5835330:0:1)$
$-13\zeta_3+39$	$(166:0:1)$	$(859:8:1)$	$(3131430:0:1)$
$1183\zeta_3-1352$	$(77:0:1)$	$(1915:1:1)$	$(4730195:0:1)$
$-1352\zeta_3-2535$	$(208:0:1)$	$(557:11:1)$	$(5835330:0:1)$

Filling in these points on the pushout forms gives the following pairing elements. Denote by $b_g^{(p)}$ the element obtained from $g \in S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ at prime p.

Selmer group element	mod $b_g^{(3)}$ mod 3^5	mod $b_g^{(13)}$ mod 13^3	mod $b_g^{(181)}$ mod 181^3
1	0	0	0
ζ_3	143	1122	855406
ζ_3+1	55	665	1854180
$-39\zeta_3-52$	189	811	5021673
$2535\zeta_3+1183$	108	460	5700414
$-52\zeta_3-13$	236	2043	1443656
$-13\zeta_3+39$	34	383	4155655
$1183\zeta_3-1352$	148	405	4801749
$-1352\zeta_3-2535$	135	2165	360371

We now use Section 3.2 to compute the local pairings. Both the primes 13 and 181 are split and we choose $p_{13} = -3\zeta_3+1$ and $p_{181} = -4\zeta_3-15$. We can then use Remark 3.2.4. The following table gives the necessary information to calculate the local pairing at 13. For the sake of brevity we include only the generators of $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$.

$(a, b_g^{(13)})_{p_{13}}$	$\mathrm{val}_{p_{13}}(a)$	$\mathrm{val}_{p_{13}}(b_g^{(13)})$	c	$\left(\frac{c}{p_{13}}\right)$
$(\zeta_3, b_{\zeta_3}^{(13)})_{p_{13}}$	0	0	1	0
$(-39\zeta_3-52, b_{\zeta_3}^{(13)})_{p_{13}}$	1	0	$1/1122$	2
$(\zeta_3, b_{-39\zeta_3-52}^{(13)})_{p_{13}}$	0	0	1	0
$(-39\zeta_3-52, b_{-39\zeta_3-52}^{(13)})_{p_{13}}$	1	0	$1/811$	0

We can repeat the calculation above for all the elements in the table. We obtain the following table for the local pairing at 13.

	1	ζ_3	ζ_3+1	$-39\zeta_3-52$	$2535\zeta_3+1183$	$-52\zeta_3-13$	$-13\zeta_3+39$	$1183\zeta_3-1352$	$-1352\zeta_3-2535$
1	0	0	0	0	0	0	0	0	0
ζ_3	0	0	0	0	0	0	0	0	0
ζ_3+1	0	0	0	0	0	0	0	0	0
$-39\zeta_3-52$	0	1	2	0	0	2	1	2	1
$2535\zeta_3+1183$	0	2	1	0	0	1	2	1	2
$-52\zeta_3-13$	0	1	2	0	0	2	1	2	1
$-13\zeta_3+39$	0	1	2	0	0	2	1	2	1
$1183\zeta_3-1352$	0	2	1	0	0	1	2	1	2
$-1352\zeta_3-2535$	0	2	1	0	0	1	2	1	2

Similarly, the following table gives the local pairing at 181.

$(a, b_g^{(181)})_{p_{181}}$	$\mathrm{val}_{p_{181}}(a)$	$\mathrm{val}_{p_{181}}(b_g^{(181)})$	c	$\left(\frac{c}{p_{181}}\right)$
$(\zeta_3, b_{\zeta_3}^{(181)})_{p_{181}}$	0	1	ζ_3	0
$(-39\zeta_3-52, b_{\zeta_3}^{(181)})_{p_{181}}$	0	1	$-39\zeta_3-52$	0
$(\zeta_3, b_{-39\zeta_3-52}^{(181)})_{p_{181}}$	0	0	1	0
$(-39\zeta_3-52, b_{-39\zeta_3-52}^{(181)})_{p_{181}}$	0	0	1	0

Thus the local pairing at 181 is given by the zero matrix. At the prime $p=3$, we must use Proposition 3.2.7. Each of the elements used lies in a class generated by $\langle \lambda, \eta_1, \eta_2, \eta_3 \rangle$. The following table gives the class for each element, after which we can use Table 3.1.

element	class	element	class
1	1	$b_1^{(3)}$	1
ζ_3	η_1	$b_1^{(3)}$	1
ζ_3+1	η_1^2	$b_{\zeta_3}^{(3)}$	1
$-39\zeta_3-52$	η_3^2	$b_{-39\zeta_3-52}^{(3)}$	$\eta_2^2\eta_3^2$
$2535\zeta_3+1183$	η_3	$b_{2535\zeta_3+1183}^{(3)}$	$\eta_2\eta_3$
$-52\zeta_3-13$	$\eta_1^2\eta_3^2$	$b_{-52\zeta_3-13}^{(3)}$	$\eta_2^2\eta_3^2$
$-13\zeta_3+39$	$\eta_1\eta_3^2$	$b_{-13\zeta_3+39}^{(3)}$	$\eta_2^2\eta_3^2$
$1183\zeta_3-1352$	$\eta_1^2\eta_3$	$b_{1183\zeta_3-1352}^{(3)}$	$\eta_2\eta_3$
$-1352\zeta_3-2535$	$\eta_1\eta_3$	$b_{-1352\zeta_3-2535}^{(3)}$	$\eta_2\eta_3$

Thus the local pairing at 3 is given by the following table.

	1	ζ_3	ζ_3+1	$-39\zeta_3-52$	$2535\zeta_3+1183$	$-52\zeta_3-13$	$-13\zeta_3+39$	$1183\zeta_3-1352$	$-1352\zeta_3-2535$
1	0	0	0	0	0	0	0	0	0
ζ_3	0	0	0	2	1	2	2	1	1
ζ_3+1	0	0	0	1	2	1	1	2	2
$-39\zeta_3-52$	0	0	0	0	0	0	0	0	0
$2535\zeta_3+1183$	0	0	0	0	0	0	0	0	0
$-52\zeta_3-13$	0	0	0	1	2	1	1	2	2
$-13\zeta_3+39$	0	0	0	2	1	2	2	1	1
$1183\zeta_3-1352$	0	0	0	1	2	1	1	2	2
$-1352\zeta_3-2535$	0	0	0	2	1	2	2	1	1

The final table for the Cassels-Tate pairing is given by adding the table for the local pairing at 3 to the table for the local pairing at 13. We therefore obtain the following table.

	1	ζ_3	ζ_3+1	$-39\zeta_3-52$	$2535\zeta_3+1183$	$-52\zeta_3-13$	$-13\zeta_3+39$	$1183\zeta_3-1352$	$-1352\zeta_3-2535$
1	0	0	0	0	0	0	0	0	0
ζ_3	0	0	0	2	1	2	2	1	1
ζ_3+1	0	0	0	1	2	1	1	2	2
$-39\zeta_3-52$	0	1	2	0	0	2	1	2	1
$2535\zeta_3+1183$	0	2	1	0	0	1	2	1	2
$-52\zeta_3-13$	0	1	2	1	2	0	2	1	0
$-13\zeta_3+39$	0	1	2	2	1	1	0	0	2
$1183\zeta_3-1352$	0	2	1	1	2	2	0	0	1
$-1352\zeta_3-2535$	0	2	1	2	1	0	1	2	0

We see from the table above that the pairing we have calculated is both skew-symmetric and bilinear, as required. As we can see, this gives us the same result as when we calculated the pairing in Example 5.1.2.

In the following two examples, we calculate the pairing only on the generators of $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ and not on the full group.

Example 5.2.2. Let E be given by $y^2 = x^3 + (x+15)^2$ as in Example 5.1.3. The relevant Selmer group is

$$S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) = \langle 2,3,5\rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^3.$$

To obtain simpler pushout forms, we use the following elements as generators of $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$. The covering curves are calculated using (3.73) and are given in the following table. Let $L = \mathbb{Q}(\zeta_3)$ and $M = \mathbb{Q}(\beta)$ where $\beta^3 + \frac{4}{3}\beta^2 + 60\beta + 900 = 0$. We also give an element ξ such that $N_{M/\mathbb{Q}}(\xi) = u$ for each $u \in S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$.

Selmer group generator	covering curve	ξ
$-2^4\cdot 103^3$	$2^9\cdot 103^6x^3-2^5\cdot 103^3+2^4\cdot 103^3y^3+30z^3=0$	$\frac{1}{15}(3\beta^2+364\beta-1200)$
$-3\cdot 47^3$	$3^2\cdot 47^6x^3-2\cdot 3\cdot 47^3xyz+3\cdot 47^3y^3+30z^3=0$	$\frac{1}{6}(-3\beta^2+32\beta-18)$
$5\cdot 31^3$	$5^2\cdot 31^6x^3+2\cdot 5\cdot 31^3xyz-5\cdot 31^3y^3+30z^3=0$	$\frac{1}{30}(21\beta^2-62\beta+1290)$

The pushout forms are calculated using Section 3.5.4 and are given in the following table. Unfortunately, the MAGMA lattice functions we used previously to simplify pushout forms are not implemented over $\mathbb{Q}(\sqrt{-3})$, therefore we leave the pushout forms in their original, ugly forms.

Selmer group generator	pushout form
$-2^4\cdot 103^3$	$(955045035851 52\zeta_3+809107610825472)x^3+3403853346816x^2y$ $+(-9070665216\zeta_3+73768190976)x^2z-13605997824xy^2$ $+\frac{1}{1092727}(168141771526224\zeta_3+73980485713920)xyz+(3499840\zeta_3+4343632)xz^2$ $+\frac{1}{1092727}(-5969031474072\zeta_3-50569225676592)y^3+(-129792\zeta_3-1525272)y^2z$ $+\frac{1}{1092727}(18516106308\zeta_3-2695730240)yz^2+\frac{1}{10746470668761}(2466440150422033\zeta_3$ $+1372243865274116)z^3$
$-3\cdot 47^3$	$\frac{1}{2}(-38549581620\zeta_3+754651776945)x^3-11567024253x^2y+(109013118\zeta_3+208241706)x^2z$ $+163519677xy^2+\frac{1}{103823}(-375837198742\zeta_3-378841668751)xyz+(185064\zeta_3+192480)xz^2$ $+\frac{1}{207646}(12849860540\zeta_3-251550592315)y^3+(24758\zeta_3+38392)y^2z$ $+\frac{1}{103823}(-294587892\zeta_3-70501072)yz^2+\frac{1}{97012937961}(11882044885654\zeta_3+3000419480357)z^3$
$5\cdot 31^3$	$\frac{1}{2}(193566948996\zeta_3+216968917965)x^3+4897193535x^2y+(7424502\zeta_3-237440922)x^2z$ $+11136753xy^2+\frac{1}{148955}(-635409568686\zeta_3-924093348075)xyz+(222780\zeta_3+319196)xz^2$ $+\frac{1}{297910}(193566948996\zeta_3+216968917965)y^3+(21918\zeta_3-100788)y^2z$ $+\frac{1}{29791}(-160166192\zeta_3-30668856)yz^2+\frac{1}{39937665645}(3416592907598\zeta_3+10575078500125)z^3$

The set of bad primes of E where the local pairing is nontrivial is

$$P=\{2,3,5,401\}$$

and this set need not be enlarged in this case (see Proposition 3.3.6). For each covering curve, we find a local point. The ones we used are given in the following table.

Selmer group element	mod 2^8	mod 3^6	mod 5^3	mod 401^3
2	$(0:135:2)$	$(443:586:3)$	$(93:1:0)$	$(34727645:0:1)$
3	$(67:1:0)$	$(126:1:1)$	$(66:1:0)$	$(10349116:0:1)$
5	$(107:1:0)$	$(40:20:3)$	$(5:1:1)$	$(2901156:0:1)$

Filling in these points on our pushout forms gives the following elements. Denote by $b_g^{(p)}$ the element obtained from generator g at prime p.

Selmer group element	$b_g^{(2)}$ mod 2^8	$b_g^{(3)}$ mod $3^?$	$b_g^{(5)}$ mod 5^3	$b_g^{(401)}$ mod 401^3
$-2^4\cdot 103^3$	$64\zeta_3+192$	$618\zeta_3+165$	$28\zeta_3+85$	$31469285\zeta_3+27598825$
$-3\cdot 47^3$	$132\zeta_3+253$	$117\zeta_3+126$	$105\zeta_3+84$	$20164293\zeta_3+31205419$
$5\cdot 31^3$	$204\zeta_3+57$	$114\zeta_3+417$	$28\zeta+115$	$44672611\zeta_3+30314798$

We now use Section 3.2 to compute the local pairing at prime 2. The following table contains the necessary information to calculate this local pairing.

$(a,b_g^{(2)})_2$	$\mathrm{val}_2(a)$	$\mathrm{val}_2(b_g^{(2)})$	c	$\left(\frac{c}{v}\right)_v$
$(-2^4\cdot 103^3, b^{(2)}_{-2^4\cdot 103^3})_2$	4	6	$\frac{1}{7^4}\left(-5\cdot 11\cdot 103^{18}\zeta_3 - 2^4\cdot 103^{18}\right)$	1
$(-3\cdot 47^3, b^{(2)}_{-2^4\cdot 103^3})_2$	0	6	$3^6\cdot 47^{18}$	0
$(5\cdot 31^3, b^{(2)}_{-2^4\cdot 103^3})_2$	0	6	$5^6\cdot 31^18$	0
$(-2^4\cdot 103^3, b^{(2)}_{-3\cdot 47^3})_2$	4	0	$\frac{1}{11^4\cdot 397^4}\left(-2^4\cdot 3\cdot 17\cdot 181\zeta_3 - 5\cdot 7\cdot 11\cdot 431\right)$	0
$(-3\cdot 47^3, b^{(2)}_{-3\cdot 47^3})_2$	0	0	1	0
$(5\cdot 31^3, b^{(2)}_{-3\cdot 47^3})_2$	0	0	1	0
$(-2^4\cdot 103^3, b^{(2)}_{5\cdot 31^3})_2$	4	0	$\frac{1}{3^6\cdot 1231^4}\left(-2^4\cdot 5\cdot 17\cdot 23\cdot 47\zeta_3 + 7^2\cdot 29\cdot 61\right)$	0
$(-3\cdot 47^3, b^{(2)}_{5\cdot 31^3})_2$	0	0	1	0
$(5\cdot 31^3, b^{(2)}_{5\cdot 31^3})_2$	0	0	1	0

Thus the local pairing at 2 is given by the following matrix.

	$-2\cdot 103^3$	$-3\cdot 47^3$	$5\cdot 31^3$
$-2\cdot 103^3$	1	0	0
$-3\cdot 47^3$	0	0	0
$5\cdot 31^3$	0	0	0

The primes 5 and 401 are also inert in L. We follow the same procedure as above to obtain the following tables.

$(a,b_g^{(5)})_5$	$\mathrm{val}_5(a)$	$\mathrm{val}_5(b_g^{(5)})$	c	$\left(\frac{c}{v}\right)$
$(-2^4\cdot 103^3, b^{(5)}_{-2^4\cdot 103^3})_5$	0	0	1	0
$(-3\cdot 47^3, b^{(5)}_{-2^4\cdot 103^3})_5$	0	0	1	0
$(5\cdot 31^3, b^{(5)}_{-2^4\cdot 103^3})_5$	1	0	$\frac{1}{10789}\left(-2^2\cdot 7 + 3\cdot 29\right)$	1
$(-2^4\cdot 103^3, b^{(5)}_{-3\cdot 47^3})_5$	0	0	1	0
$(-3\cdot 47^3, b^{(5)}_{-3\cdot 47^3})_5$	0	0	1	0
$(5\cdot 31^3, b^{(5)}_{-3\cdot 47^3})_5$	1	0	$\frac{1}{3^2\cdot 7^2}\left(-5\zeta_3 - 1\right)$	0
$(-2^4\cdot 103^3, b^{(5)}_{5\cdot 31^3})_5$	0	0	1	0
$(-3\cdot 47^3, b^{(5)}_{5\cdot 31^3})_5$	0	0	1	0
$(5\cdot 31^3, b^{(5)}_{5\cdot 31^3})_5$	1	0	$\frac{1}{10789}\left(-2^2\cdot 7\zeta_3 + 3\cdot 29\right)$	1

$(a, b_g^{(401)})_{401}$	$\mathrm{val}_{401}(a)$	$\mathrm{val}_{401}(b_g^{(401)})$	c	$\left(\frac{c}{v}\right)$
$(-2^4\cdot 103^3, b^{(401)}_{-2^4\cdot 103^3})_{401}$	0	0	1	0
$(-3\cdot 47^3, b^{(401)}_{-2^4\cdot 103^3})_{401}$	0	0	1	0
$(5\cdot 31^3, b^{(401)}_{-2^4\cdot 103^3})_{401}$	0	0	1	0
$(-2^4\cdot 103^3, b^{(401)}_{-3\cdot 47^3})_{401}$	0	0	1	0
$(-3\cdot 47^3, b^{(401)}_{-3\cdot 47^3})_{401}$	0	0	1	0
$(5\cdot 31^3, b^{(401)}_{-3\cdot 47^3})_{401}$	0	0	1	0
$(-2^4\cdot 103^3, b^{(401)}_{5\cdot 31^3})_{401}$	0	0	1	0
$(-3\cdot 47^3, b^{(401)}_{5\cdot 31^3})_{401}$	0	0	1	0
$(5\cdot 31^3, b^{(401)}_{5\cdot 31^3})_{401}$	0	0	1	0

Thus the local pairing on 401 is the zero matrix and the local pairing at 5 is given by

	$-2\cdot 103^3$	$-3\cdot 47^3$	$5\cdot 31^3$
$-2\cdot 103^3$	0	0	0
$-3\cdot 47^3$	0	0	0
$5\cdot 31^3$	1	0	1

For the prime 3, we must use Proposition 3.2.7. Each of the elements lies in a class generated by $\langle \lambda, \eta_1, \eta_2, \eta_3 \rangle$. The following table gives the class for each element, after which we can use Table 3.1.

element	class	element	class
$-2^4\cdot 103^3$	$\eta_2^2\eta_3^2$	$b^{(3)}_{-2^4\cdot 103^3}$	$\eta_1^2\eta_3$
$-3\cdot 47^3$	$\lambda^2\eta_1^2$	$b^{(3)}_{-3\cdot 47^3}$	$\lambda^2\eta_1\eta_2\eta_3$
$5\cdot 31^3$	$\eta_2\eta_3$	$b^{(3)}_{5\cdot 31^3}$	$\eta_1\eta_2^2\eta_3$

Thus the local pairing at 3 is given by the following matrix.

	$-2\cdot 103^3$	$-3\cdot 47^3$	$5\cdot 31^3$
$-2\cdot 103^3$	2	2	1
$-3\cdot 47^3$	1	0	2
$5\cdot 31^3$	1	1	2

We now have all the information we need to use Definition 3.3.2. We can add the local pairing computed together to obtain the following matrix for the Cassels-Tate pairing.

	2	3	5
2	0	2	1
3	1	0	2
5	2	1	0

We see that this is the same as the result obtained in Example 5.1.3.

We now do an example we did not see in the previous section.

Example 5.2.3. Let E be the elliptic curve given by the Cremona reference 124656dp1. Thus

$$E : y^2 = x^3 + 7(x+3)^2$$

This is a curve of type `Generic3Isogeny`. The points of order 3 are generated by $S = (0, 3\sqrt{7})$ and $T = \left(\beta, \sqrt{7}\left(\left(\frac{2}{3}\zeta_3 + \frac{1}{3}\right)\beta + 6\zeta_3 + 3\right)\right)$ where β satisfies $\beta^3 + \frac{28}{3}\beta^2 + 84\beta + 252 = 0$. Let $\phi : E \to \hat{E}$ be the isogeny with kernel $\langle S \rangle$ and the isogenous curve given by

$$\hat{E} : y^2 = x^3 - 21\left(x + \frac{53}{9}\right)^2.$$

The Selmer groups are given by

$$S^{(\phi)}(E/\mathbb{Q}) = \langle 1 \rangle \subset \mathbb{Q}(\sqrt{-21})^\times/(\mathbb{Q}(\sqrt{-21}))^3$$
$$S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) = \langle 6\sqrt{7} - 6, 2\sqrt{7} - 6 \rangle \subset \mathbb{Q}(\sqrt{7})^\times/(\mathbb{Q}(\sqrt{7}))^3.$$

Thus an initial estimate for the rank of this curve is 2. The covering curves are given by (3.78) and are displayed in the following table. We choose generators for $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ so that our pushout forms may be as small as possible. Let $g_1 = -7434691125 - 2809798500\sqrt{7}$ and $g_2 = -12356000 - 4691000\sqrt{7}$.

Selmer group element	covering curve
g_1	$936599500x^3 - 7434691125x^2y + 71475x^2z + 19668589500xy^2$ $-17347612625y^3 - 500325y^2z + z^3 = 0$
g_2	$4691000x^3 - 37068000x^2y - 11100x^2z + 98511000xy^2$ $-86492000y^3 + 77700y^2z + 3z^3 = 0$

The pushout forms are found using Section 3.5.3.

Selmer group element	pushout form
g_1	$(-40333598716084562480900\sqrt{-21} + 2699010887195620714649 25)x^3$ $+(32832051384094103483580 0\sqrt{-21} - 2020863599183663826602850)x^2y$ $+(-175096477981304721435\sqrt{-21} - 553009343563125115380)x^2z$ $+(-89142036083291599770390 0\sqrt{-21} + 4985841960309190994998425)xy^2$ $+(952129185103164978000\sqrt{-21} + 3200284732746452904000)xyz$ $+(-67522868503646850\sqrt{-21} - 43477402706488800)xz^2$ $+(80694473366362952711020 0\sqrt{-21} - 4042268562540908638651650)y^3$ $+(-129021726420410499595 5\sqrt{-21} - 4567253877421251545340)y^2z$ $+(186511783405172400\sqrt{-21} - 189087354099652050)yz^2$ $+(-217589284409765\sqrt{-21} + 1100767370166030)z^3$
g_2	$(-211818042536960\sqrt{-21} - 5703361793598080)x^3$ $+(-140702811594240\sqrt{-21} + 41773050139755480)x^2y$ $+(14250174188484\sqrt{-21} - 4424758732968)x^2z$ $+(4222120240611840\sqrt{-21} - 97479547173415680)xy^2$ $+(-63083483769600\sqrt{-21} + 13925835025200)xyz$ $+(147087605160\sqrt{-21} + 464150305080)xz^2$ $+(-6295225908146560\sqrt{-21} + 72747675328616120)y^3$ $+(69838795705812\sqrt{-21} - 36027019071624)y^2z$ $+(-424469785320\sqrt{-21} - 1632955849560)yz^2$ $+(-880889043\sqrt{-21} + 3138851436)z^3$

We found some local points on each of our covering curves. The bad primes to be considered are $P = \{2,3,7,53\}$, and this set must be enlarged to $P = \{2,3,5,7,53\}$ in this case (see Proposition 3.3.6). The local points we used are given in the following table.

	mod 2^6	mod 3^6	mod 5^5	mod 7^3	mod 53^3
g_1	$(55:4:0)$	$(145:583:1)$	$(2767:0:5)$	$(171:0:1)$	$(105550:0:1)$
g_2	$(0:3:8)$	$(199:265:9)$	$(0:1651:5)$	$(185:1:0)$	$(71049:0:1)$

Filling these in on our pushout forms gives the following pairing elements. Let $b_g^{(p)}$ denote the element obtained from generator g, at prime p.

	mod 2^6	mod 3^6	mod 5^5	mod 7^3	mod 53^3
g_1	$19+4\sqrt{-21}$	$621+594\sqrt{-21}$	$550+1600\sqrt{-21}$	$167+70\sqrt{-21}$	$115306+6898\sqrt{-21}$
g_2	$40+32\sqrt{-21}$	$702+702\sqrt{-21}$	$2750+1375\sqrt{-21}$	$241+146\sqrt{-21}$	$145521+1629\sqrt{-21}$

We now use Section 3.2 to compute the local pairing at prime 2. This prime is inert in $\mathbb{Q}(\zeta_3)$. By Remark 3.2.1, we must extend $\mathbb{Q}(\zeta_3)_2$ by adding $\sqrt{7}$. To recover the actual answer, we must then multiply the final answer by 2. Let $p_2 = -\zeta_3\sqrt{7} - 3\zeta_3$, the only prime lying over 2 in $\mathbb{Q}(\zeta_3, \sqrt{7})$. The following table contains the necessary information to calculate this local pairing.

$(a, b_g^{(2)})_{p_2}$	$\mathrm{val}_{p_2}(a)$	$\mathrm{val}_{p_2}(b_g^{(2)})$	c	$\left(\frac{c}{p_2}\right)$
$(g_1, b_{g_1}^{(2)})_{p_2}$	0	0	1	0
$(g_2, b_{g_1}^{(2)})_{p_2}$	6	0	$\left(\frac{1}{b_{g_1}^{(2)}}\right)^6$	0
$(g_1, b_{g_2}^{(2)})_{p_2}$	0	6		0
$(g_2, b_{g_2}^{(2)})_{p_2}$	6	6		0

Thus the local pairing at 2 is given by the zero matrix. The primes 5 and 53 are also inert in $\mathbb{Q}(\zeta_3)$. As in the 2 case, we extend $\mathbb{Q}(\zeta_3)_5$ by adding $\sqrt{7}$ and multiply the final answer by 2. However, there is a root of 7 in $\mathbb{Q}(\zeta_3)_{53}$, therefore this need not be done. The prime 7 is split in $\mathbb{Q}(\zeta_3)$, therefore we must multiply the final answer by 2. However, we must also extend $\mathbb{Q}_7$ by adding $\sqrt{7}$, therefore, we must multiply the final answer by 4 in total.

$(a, b_g^{(2)})_{p_5}$	$\mathrm{val}_{p_5}(a)$	$\mathrm{val}_{p_5}(b_g^{(2)})$	c	$\left(\frac{c}{p_5}\right)$
$(g_1, b_{g_1}^{(5)})_{p_5}$	3	2	$\frac{g_1^2}{\left(b_{g_1}^{(5)}\right)^3}$	2
$(g_2, b_{g_1}^{(5)})_{p_5}$	3	2	$\frac{g_2^2}{\left(b_{g_1}^{(5)}\right)^3}$	1
$(g_1, b_{g_2}^{(5)})_{p_5}$	3	5	$-\frac{g_1^5}{\left(b_{g_2}^{(5)}\right)^3}$	2
$(g_2, b_{g_2}^{(5)})_{p_5}$	3	5	$-\frac{g_2^5}{\left(b_{g_2}^{(5)}\right)^3}$	1

$(a, b_g^{(7)})_{p_7}$	$\mathrm{val}_{p_7}(a)$	$\mathrm{val}_{p_7}(b_g^{(7)})$	c	$\left(\frac{c}{p_7}\right)$
$(g_1, b_{g_1}^{(7)})_{p_7}$	0	0	1	0
$(g_2, b_{g_1}^{(7)})_{p_7}$	0	0	1	0
$(g_1, b_{g_2}^{(7)})_{p_7}$	0	0	1	0
$(g_2, b_{g_2}^{(7)})_{p_7}$	0	0	1	0

$(a, b_g^{(2)})_{p_{53}}$	$\mathrm{val}_{p_{53}}(a)$	$\mathrm{val}_{p_{53}}(b_g^{(53)})$	c	$\left(\frac{c}{p_{53}}\right)$
$(g_1, b_{g_1}^{(53)})_{p_{53}}$	0	0	1	0
$(g_2, b_{g_1}^{(53)})_{p_{53}}$	0	0	1	0
$(g_1, b_{g_2}^{(53)})_{p_{53}}$	0	0	1	0
$(g_2, b_{g_2}^{(53)})_{p_{53}}$	0	0	1	0

Thus the local pairings at 7 and 53 are given by the zero matrix, and the local pairing at 5 is given by

	g_1	g_2
g_1	1	1
g_2	2	2

We now move on to the prime 3, for which we use Proposition 3.2.7. Each element lies in a class generated by $\langle \lambda, \eta_1, \eta_2, \eta 3 \rangle$, and the following table shows which one it is for each element. Next to it is the matrix obtained by calculating the local pairing, which we did using Table 3.1.

element	class	element	class
g_1	$\lambda\eta_1$	$b_{g_1}^{(3)}$	$\eta_1^2\eta_3$
g_2	$\eta_2^2\eta_3^2$	$b_{g_2}^{(3)}$	$\eta_1\eta_2^2\eta_3$

	g_1	g_2
g_1	2	1
g_2	2	1

We can now use Definition 3.3.2 to find the following matrix giving us the Cassels-Tate pairing on $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$. It is obtained by adding the local pairing for 3 to the local pairing for 5.

	g_1	g_2
g_1	0	2
g_2	1	0

Thus we find that the rank of E must be 0, and $Ш(E/\mathbb{Q})[\phi] \cong (\mathbb{Z}/3\mathbb{Z})^2$.

The difference between using either the direct Weil pairing method or the pushout form method depends mostly on whether we want to compute local points on E itself or on the coverings of E. However, we see some advantages to using the pushout form method. Namely the local points, when found, are not manipulated to quite the same extent, making it easier to choose the degree of accuracy to work to. Also, in step 6 of Procedure 5.1.1, we must find local points satisfying some requirement, whereas when we search for local points in the pushout form method, almost any local point will do, which makes it easier to select a suitable point. The pushout form may look rather nasty, but when doing calculations it is very easy to use. The pushout form method also generalises quite nicely, as we see in Chapters 7 and 8.

Chapter 6

High Rank Elliptic Curves Having Prescribed Torsion Group

In this chapter, we consider several different families of elliptic curves over $\mathbb{Q}$. The first family consists of curves E with torsion group $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. There are five known curves in this family with rank at least 13. We show that the rank cannot be higher in any of these cases. The other two families we consider will have torsion groups isomorphic to $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$ respectively, and we seek high rank curves in each of these families.

All norm equations in this chapter were calculated using the theory set out in Chapter 4. Either MAGMA's function `NormEquation` was avoided altogether or the problem was reduced until `NormEquation` could be used. In fact, all but a select few could not have been calculated without it, and even where `NormEquation` would have sufficed, we often found a solution with smaller coefficients.

In each family, let E be a curve and let $\phi : E \to \hat{E}$ be a 3-isogeny with kernel generated by $S \in E[3]$, a 3-torsion point defined over $\mathbb{Q}$. We calculate the Selmer group $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ as a subgroup of $\mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^3$ and calculate the Cassels-Tate pairing on it using the pushout form definition, namely Definition 3.3.2. We also calculate the size of $S^{(\phi)}(E/\mathbb{Q})$ using a formula of Cassels [Cas65].

$$\frac{\#S^{(\phi)}(E/\mathbb{Q})}{\#S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})} = \frac{\#E(\mathbb{Q})[\phi]}{\#\hat{E}(\mathbb{Q})[\hat{\phi}]} \cdot \frac{\Omega'}{\Omega} \cdot \prod_p \frac{c_p'}{c_p} \tag{6.1}$$

Here, c_p are the Tamagawa numbers and $\Omega = \int_{E(\mathbb{R})} \omega$ for ω the canonical Néron differential of E. It is calculated in [Del08] that, if E is given in the form $y^2 = x^3 + \Delta(\varepsilon x + \eta)^2$, then

$$\Omega = \begin{cases} \Omega', & \text{if } \Delta < 0 \\ 3\Omega' & \text{if } \Delta > 0 \end{cases}. \tag{6.2}$$

In all our examples in this section, we will have $\Delta = 1$. Thus we obtain

$$\frac{\#S^{(\phi)}(E/\mathbb{Q})}{\#S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})} = \prod_p \frac{c_p'}{c_p}.$$

Recall from Section 2.7 that the rank r_E of E is given by

$$3^{r_E} = \frac{|S^{(\phi)}(E/\mathbb{Q})| \cdot |S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})|}{3 \cdot |Ш(E/\mathbb{Q})[\phi]| \cdot |Ш(\hat{E}/\mathbb{Q})[\hat{\phi}]|} \tag{6.3}$$

and the rank approximation (2.34)

$$3^{r_E} \leq \frac{|S^{(\phi)}(E/\mathbb{Q})| \cdot |S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})|}{3 \cdot 3^{\mathrm{Rank}(\hat{M})}} \tag{6.4}$$

where $\hat{M}$ is the matrix representing the Cassels-Tate pairing on $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$.

The families of curves we look at in this chapter will all have a specified torsion group over $\mathbb{Q}$. We follow Kubert [Kub76], who gave parametrisations for all families of curves mentioned in Theorem 2.1.3. The three families of interest will be those with torsion groups $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$. We recall the *Tate Normal form*, or *Kubert curve*, first suggested by Tate in [Tat74].

Theorem 6.0.1. *Every elliptic curve E with a rational point of order $n = 4, \ldots, 12$ can be written in the* Tate Normal Form

$$E(b,c) : y^2 + (1-c)xy - by = x^3 - bx^2$$

with $P = (0,0)$ a point of order n.

Reichert tabulated small powers of the point $P = (0,0)$ in [Rei86], up to $6P$. We expanded this list to obtain the following.

$$\begin{aligned}
P &= (0,0) \\
2P &= (b,bc) \\
3P &= (c,b-c) \\
4P &= (d(d-1), d^2(c-d+1)); && b = cd \\
5P &= (de(e-1), de^2(d-e)); && c = e(d-1) \\
6P &= (-fg, f^2(f+2g-1)); && f(1-e) = e(1-d) \text{ and } d-e = g(1-e) \\
x(8P) &= \frac{d(d-1)(d-e)(d-e^2+e-1)}{(de-2d+1)^2}
\end{aligned}$$

(Note that we have corrected a slight typographical error in the expression for $4P$.) We also have

$$\begin{aligned}
-P &= (0,b) \\
-2P &= (b,0) \\
-3P &= (c,c^2) \\
-4P &= (d(d-1), d(d-1)^2).
\end{aligned}$$

Proposition 6.0.2. *Any elliptic curve with a rational 9-torsion point is isomorphic to a curve of the form*

$$E_9(s,t) : y^2 + (t^3 + s^2t - s^3)xy + (s^2t^7 - 2s^3t^6 + 2s^4t^5 - s^5t^4)y = x^3 + (s^2t^4 - 2s^3t^3 + 2s^4t^2 - s^5t)x^2$$

with $s,t \in \mathbb{Z}$. The discriminant is given by $s^9t^9(s-t)^9(s^2-st+t^2)^3(s^3-6s^2t+3st^2+t^3)$. Such a curve can also be written in the form

$$y^2 + xy + \lambda y = x^3$$

where

$$\lambda = \frac{s^6t^3 - 3s^5t^4 + 3s^4t^5 - s^3t^6}{s^9 - 9s^8t + 27s^7t^2 - 24s^6t^3 - 18s^5t^4 + 27s^4t^5 + 3s^3t^6 - 9s^2t^7 + t^9}.$$

Proof. Following [Hus04], we set $5P = -4P$. Thus from the x-coordinate we obtain

$$\begin{aligned} d(d-1) &= de(e-1) \\ d-1 &= e(e-1) \\ d &= e^2 - e + 1 \end{aligned}$$

and so we obtain

$$\begin{aligned} c &= e(d-1) = e^3 - e^2 \\ b &= cd = e^5 - 2e^4 + 2e^3 - e^2. \end{aligned}$$

Now let $e = \frac{s}{t}$ with $s,t \in \mathbb{Z}$ to obtain

$$\begin{aligned} c &= \frac{s^3}{t^3} - \frac{s^2}{t^2} \\ b &= \frac{s^5}{t^5} - 2\frac{s^4}{t^4} + 2\frac{s^3}{t^3} - \frac{s^2}{t^2}. \end{aligned}$$

By substituting these into the equation for $E(b,c)$ from Theorem 6.0.1 and then letting $y \mapsto \frac{1}{t^9}y$ and $x \mapsto \frac{1}{t^6}x$ we obtain the proposition. □

Proposition 6.0.3. *Any elliptic curve with a rational 12-torsion point is isomorphic to a curve of the form*

$$\begin{aligned} E_{12}(s,t) \; : y^2 &+ (s^4 + 2s^3t + 2s^2t^2 + 2st^3 - t^4)xy \\ &+ (-s^7t^5 - s^6t^6 - s^5t^7 + s^3t^9 + s^2t^{10} + st^{11})y \\ &= x^3 + (-s^6t^2 - 2s^5t^3 - 3s^4t^4 - 3s^3t^5 - 2s^2t^6 - st^7)x^2 \end{aligned}$$

with $s,t \in \mathbb{Z}$. The discriminant is given by $s^{12}t^{12}(s-t)^2(s+t)^6(s^2+t^2)^3(s^2+st+t^2)^4(s^2+4st+t^2)$.

Proof. The proof is similar to that of Proposition 6.0.2. We set $8P = -4P$. □

6.1 Torsion Group $\mathbb{Z}/3\mathbb{Z}$ over $\mathbb{Q}$

The highest rank found so far for an elliptic curve of prescribed torsion $\mathbb{Z}/3\mathbb{Z}$ is 13. Between 2007 and 2009, Y.G. Eroshkin discovered 5 curves with 13 independent nontorsion points. These curves can all be found on A. Dujella's website [Duj15], together with the independent points found on them. In this section we will show that none of these curves can have rank larger than 13. Let the curves in this section be expressed as in Section 2.6 as follows.

$$E_\lambda : y^2 + xy + \lambda y = x^3$$

All Selmer groups in this section were calculated using the formulae provided in [Fis03], which have been recalled in Section 2.6.

Example 6.1.1. In two cases, a descent by 3-isogeny suffices to show these curves have rank at most 13. In the table below, the first column gives the value of the parameter λ, the second a basis for $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ as a $\mathbb{F}_3$-vector space in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^3$. The third column gives the dimension of this vector space.

λ	$S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$	dim
$\frac{2^5\cdot3^3\cdot5^2\cdot7^2\cdot11^2\cdot13\cdot19\cdot23\cdot29\cdot31\cdot37\cdot41\cdot43\cdot47\cdot53\cdot61\cdot67}{17^2\cdot271^3\cdot1825933^3}$	$\langle 7\cdot11\cdot47, 11\cdot43, 11\cdot13^2\cdot61, 3\cdot7\cdot11^2\cdot13^2\cdot67,$ $7^2\cdot53, 7^2\cdot11^2\cdot41, 3\cdot7^2\cdot11\cdot13\cdot31, 11^2\cdot13\cdot37,$ $3^2\cdot13^2\cdot29, 3^2\cdot7\cdot11\cdot13^2\cdot23, 5\cdot7^2\cdot13,$ $3\cdot11^2\cdot13\cdot19, 2\cdot3\cdot11\cdot13^2, 7\cdot11^2\cdot13^2\cdot17\rangle$	14
$-\frac{2^5\cdot3^3\cdot5^2\cdot7^2\cdot11^2\cdot13\cdot17\cdot19\cdot23\cdot29\cdot31\cdot41\cdot43\cdot47\cdot53\cdot59\cdot61\cdot67}{37^2\cdot131^3\cdot3966113^3}$	$\langle 2^2\cdot5\cdot13^2\cdot17\cdot43, 2\cdot3^2\cdot5^2\cdot17\cdot67, 3\cdot13\cdot61,$ $2^2\cdot3\cdot13^2\cdot59, 2^2\cdot5^2\cdot17^2\cdot53, 3\cdot17^2\cdot41, 3\cdot13^2\cdot47,$ $2\cdot3^2\cdot5\cdot13\cdot31, 2\cdot3\cdot5^2\cdot13\cdot29, 2^2\cdot3\cdot5^2\cdot13\cdot19,$ $2^2\cdot3^2\cdot13\cdot17\cdot23, 3\cdot5^2\cdot11, 2\cdot7, 2^2\cdot3\cdot13^2\cdot37\rangle$	14

In both these cases, we see that $\prod_p \frac{c_p'}{c_p} = \frac{1}{3^{14}}$, therefore by Cassels' formula, $S^{(\phi)}(E/\mathbb{Q})$ is trivial. Thus the rank can be at most 13.

In the following three examples, we compute the Cassels-Tate pairing using Definition 3.3.2. Unfortunately, the pushout forms we computed had coefficients that were far too large to put into print. Therefore, in Section 3.5.4 we provide formulae to calculate the covering curves and pushout forms in each case. The formulae use certain parameters which we shall give the values for here. Two such parameters are the values ε and η, when we write the curve in the form

$$E_{\varepsilon,\eta} : y^2 = x^3 + (\varepsilon x + \eta)^2.$$

Example 6.1.2. Let

$$E : y^2 + xy = x^3 - 560715933702165990261993692150795879540x$$
$$+52994280301716629628978677583090036935984301286744035396 00$$

If we write this curve in the form $E_{\varepsilon,\eta}$, we get $\varepsilon = 30464882157$, and $\eta = -72141925267954214 76354328483200$. Then $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ is the subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^3$ generated by the 18 generators

$$\langle 2, 5, 11, 31, 2\cdot17, 53, 3\cdot19, 3^2\cdot7, 3\cdot29, 7\cdot13, 5\cdot47, 2\cdot3\cdot41, 2\cdot3\cdot43, 7\cdot37, 3\cdot113, 19\cdot61, 19^2\cdot59, 7^2\cdot23^2\rangle.$$

By Cassels' formula, $S^{(\phi)}(E/\mathbb{Q})$ is trivial. To use the formula in Section 3.5.4, we need the following information. We have the number fields $L_1 = \mathbb{Q}(\zeta)$ and $M = \mathbb{Q}(\zeta_3, \beta)$ where

$$\beta^3 = 197\cdot317\cdot3313949\cdot2831657657\cdot4864617187.$$

The torsion group $E[3]$ is generated by the points S and T where

$$S = (0, -72141925267954214 76354328483200)$$
$$T = (-4\beta^2 - 40619842876\beta - 412492908817731987844,$$
$$\sqrt{-3}\,(-40619842876\beta^2 - 4124929088177319878 44\beta - 1140304181270553854357 9933983036)).$$

For each of our generators u, we now need ξ such that $N_{M/L_1}(\xi) = u$. In fact, in this case we may calculate the norm equation over base field $\mathbb{Q}$ rather than L_1. This element ξ need only be known up to cubes. The following table gives such an element for each generator. In fact doing the calculation for only the first five generators is sufficient to prove the result, but we include them all for completeness' sake. Note that the generator is only accurate up to cubes. To use the formula in Section 3.5.4, the norm of the element ξ must be used instead of u itself.

Generator	ξ
2	$-12791661167108901195083383708204723739606398204193807777700\beta^2$ $-35974780275129337994447006825285487950081570761578181913750367290616 2\beta$ $+34834209910010018710057210905433683776661272848186727738790219363810045545993074$
5	$-12871396963681865059070892176009921604\beta^2$ $-42692717548276970299550600161356311247921723744\beta$ $+44376973596976054087794572384100048862928277123182966340$
11	$-37362815689074099063488833354604216628599214884972424480252219 0\beta^2$ $+78050272722730936162781273480966932685433612118847337757129830325230966592\beta$ $+90322073763801829115864422707163028415439947062451764324921299061299200585386713561$
31	$-44309491311311185791855775708339093265903879590\beta^2$ $+27222747686371971329577476282324045920938632320718377 92\beta$ $+20272776755188769514278967300578047461590115299433610386578702257645$
$2\cdot 17$	$-63718379772525878373546760904814335048392665384488\beta^2$ $-15948287088723768383807013869785160787873514948361604309214 2\beta$ $-19065516425507224591254063990024397311766291052588239154837580348491462$
53	$20156656199530289627878920682605357764144436968444009910 03\beta^2$ $-75800792783212973957308726326617247279827374941815993284159788452 67\beta$ $-31271447100841691802087173874554595659989089562158668003654297073274297692770 2$
$3\cdot 19$	$54912395169295464674794176825207841921275793321491053932460402336 0\beta^2$ $+24079890342369705457246923326544140987546302658019353354049167412083289637986\beta$ $+35869897623109804623196420116453392573228236041082563231519875575872911157530055099770 5$
$3^2\cdot 7$	$-54646936943132608402184952322821985034199729624727368398874502 8\beta^2$ $+22547074166696131710828285428907498939927492189883622973939864154219912905\beta$ $+33049421276344537523447944290141402335152555620304923820331516439320055464549298606 6$
$3\cdot 29$	$-12527048365872790226525479363572758315965684821247039092\beta^2$ $+27364140108745229489570972005008690746769994756942494811984405257 0\beta$ $-30460279663057206094979296140549067660563538784063653412646847769102622886 35$
$7\cdot 13$	$-25443745024755719001344260478905683672901503797372644895591 40\beta^2$ $+11183175813724815289980670175778492346568261475134305429437206439209227 2\beta$ $-10240659080272901181428468418862362147964659669047563995485197085119371914942822 81$
$5\cdot 47$	$-23999892564846363559024715536013741640407322623255344297251966625269078\beta^2$ $-11603192887587218729729419729353008306570323300413585877401741957571892571890880 0\beta$ $+89977342556786562748392969497257091985993905366496900958248289010555652469563246750890367 73$
$2\cdot 3\cdot 41$	$-51897721063473798696693682510966474805572694158750289701258195944\beta^2$ $+16857671315588589112239350935040016317687620959042923428535251508461189989 03\beta$ $+36828825252437202794560973174886335660511625357734731779357710345524394381305513453649$
$2\cdot 3\cdot 43$	$-95973433479198314390966800679243244151533561296942037 60\beta^2$ $+66988908412293354525802567282739854301849730262450443040553528 25\beta$ $-24167476585619940891137897236090929062094641256335859839455659884434420619 01$
$7\cdot 37$	$-61934184014425370955909556854547545775962425358565232620363984 84\beta^2$ $-45816990213976304062829084495428624008096487229317079627165642326366983676 8\beta$ $-11369890390033816133524760892841079383061469144456354453933143488166346144232582961836$
$3\cdot 113$	$-10329101979901889063298644226124776627201856841170580931851281 60\beta^2$ $-19281529433441426098400387047403238731068729462632252959720440028437915298 7\beta$ $+12076727158549042498306547245004117544980841088870847211532758893389603031079020546760$
$19\cdot 61$	$-72835492468420346365595406498996737213936237052473670148075036832115589949 4\beta^2$ $+11681750342225181278695194416646350152148381619955478694782352206881616740638713546684\beta$ $+19434520665024479760624553051458512390446503296652101005388079928110309107329981009151119353419$
$19^2\cdot 59$	$20945161102677573451367732674824596750279253761716740826935603\beta^2$ $+50518929621045124859224162507127928208741223717382070516463202173377644\beta$ $+60465815194977871629472615222209227478608696950225107911238816651987468711452129 4$
$7^2\cdot 23^2$	$12329949397240906893772449215411500314815048289124426081717323258151044\beta^2$ $-49103392447122940968657414980806315820118498797527337894792760426843129120026404 5\beta$ $+49536553721542521448994656112505055599974609710284705983986346160643445736660909989998657 40$

The bad set of primes over which we need to take the sum of local pairings is

$$P = \{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,\\ 61,113,197,317,3313949,2831657657,4864617187\}.$$

We obtain the following 18×18 matrix for the Cassels-Tate pairing.

	2	5	11	31	$2\cdot17$	53	$3\cdot19$	$3^2\cdot7$	$3\cdot29$	$7\cdot13$	$5\cdot47$	$2\cdot3\cdot41$	$2\cdot3\cdot43$	$7\cdot37$	$3\cdot113$	$19\cdot61$	$19^2\cdot59$	$7^2\cdot23^2$
2	0	0	1	2	2	2	2	2	0	0	2	2	0	0	1	2	0	2
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	2	0	0	0	1	2	1	0	2	1	1	0	2	1	1	1	1	0
31	1	0	0	0	1	1	1	2	1	0	0	2	2	1	2	1	0	0
$2\cdot17$	1	0	2	2	0	1	2	1	1	0	0	0	0	2	2	1	0	2
53	1	0	1	2	2	0	2	0	1	1	0	0	0	0	0	2	1	2
$3\cdot19$	1	0	2	2	1	1	0	2	1	2	2	1	2	0	2	2	2	2
$3^2\cdot7$	1	0	0	1	2	0	1	0	1	0	2	2	0	2	0	0	0	1
$3\cdot29$	0	0	1	2	2	2	2	2	0	0	2	2	0	0	1	2	0	2
$7\cdot13$	0	0	2	0	0	2	1	0	0	0	2	1	2	2	1	2	0	0
$5\cdot47$	1	0	2	0	0	0	1	1	1	1	0	2	2	2	0	2	1	0
$2\cdot3\cdot41$	1	0	0	1	0	0	2	1	1	2	1	0	2	0	0	1	2	1
$2\cdot3\cdot43$	0	0	1	1	0	0	1	0	0	1	1	1	0	1	0	2	1	1
$7\cdot37$	0	0	2	2	1	0	0	1	0	1	1	0	2	0	0	2	1	2
$3\cdot113$	2	0	2	1	1	0	1	0	2	2	0	0	0	0	0	1	2	1
$19\cdot61$	1	0	2	2	2	1	1	0	1	1	1	2	1	1	2	0	1	2
$19^2\cdot59$	0	0	2	0	0	2	1	0	0	0	2	1	2	2	1	2	0	0
$7^2\cdot23^2$	1	0	0	0	1	1	1	2	1	0	0	2	2	1	2	1	0	0

This matrix has rank 4, thus we have found 4 nontrivial generators of $Ш(\hat{E}/\mathbb{Q})[\hat{\phi}]$. By the rank estimate (6.3), the rank must now satisfy

$$3^{r_E} \leq \frac{3^{18}\cdot 3^0}{3\cdot 3^4\cdot 3^0}$$

and hence

$$r_E \leq 13.$$

However, we already know 13 independent points on the curve, thus the rank is precisely 13.

Example 6.1.3. Let

$$E : y^2 + xy = x^3 - 3582219213057278420648051429623990891942 5x\\ +260971956875062006545492392139176746160432482417574129745 5625.$$

This curve is isomorphic to $E_{\varepsilon,\eta}$ where $\varepsilon = 106289446047$ and $\eta = -182589297580839870994454685504 00$. Then $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ is the subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^3$ generated by the 16 elements

$$\langle 2\cdot13, 29, 47, 2^2\cdot3\cdot5, 3^2\cdot7, 2\cdot3\cdot11, 2\cdot41, 2\cdot3\cdot23, 3^2\cdot19, 2\cdot3\cdot31,\\ 2^2\cdot59, 2\cdot3\cdot43, 2\cdot3^2\cdot17, 2\cdot3^2\cdot53, 2^2\cdot3^2\cdot37, 2^2\cdot3\cdot31^2\cdot61\rangle.$$

By Cassels' formula, $S^{(\phi)}(E/\mathbb{Q})$ is trivial, thus the upper bound on the rank is 15. All we need to do in this example to show the rank is actually 13 is to show that one of our generators has a nontrivial pairing with some other element. We chose this generator carefully to give us the nicest possible pushout form to work with. Let us consider the generator $2\cdot 13$. The covering curve is

$$676x^3 + 5527051194444xyz - 26y^3 - 365178595161679741988909371008 00z^3 = 0$$

and the pushout form is

$$520x^3 + 1014x^2y + (-1381762798611\sqrt{-3} - 1381762798611)x^2z + 39xy^2 + (-1381762798611\sqrt{-3} + 106289446047)xyz + (9791120162181040736047 8\sqrt{-3} + 9791120162181040736047 8)xz^2 + 19y^3 + (-1381762798611\sqrt{-3} + 1381762798611)y^2z + (-3765815446992707975403\sqrt{-3} + 3765815446992707975403)yz^2 + (-16876672968810939434095449753 8996\sqrt{-3} - 7022665291570764269017487904 00)z^3.$$

The set of bad primes of E is

$$P = \{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,187172595299,7081017707425445923\}.$$

For each such prime, we need a local point on the covering curve.

p	Local Point on C, mod p^3
2	$(2:2:1)$
3	$(16:43:9)$
5	$(76:1:0)$
7	$(185:3:1)$
11	$(262:1:0)$
13	$(1089:10:1)$
17	$(3238:1:0)$
19	$(1449:1:0)$
23	$(6741:1:0)$
29	$(20859:1:0)$
31	$(4288:10:1)$
37	$(27572:1:0)$
41	$(8932:1:0)$
43	$(17489:31:1)$
47	$(9697:1:0)$
53	$(121087:1:0)$
59	$(125922:1:0)$
61	$(87922:21:1)$
187172595299	$(10795596247519328665183243241 83386:0:1)$
7081017707425445923	$(19684693842879206271381135231428059803765234125343530 1098:0:1)$

Although it is unnecessary for the conclusion, we calculated the above for each generator to obtain the full matrix. This not only did not significantly increase the time needed for the calculation, but also provided a useful check that the calculation was indeed correct. We obtain the following 16×16 matrix, and the covering curve and pushout form shown above give us the first row of this matrix.

	$2\cdot13$	29	47	$2^2\cdot3\cdot5$	$3^2\cdot7$	$2\cdot3\cdot11$	$2\cdot41$	$2\cdot3\cdot23$	$3^2\cdot19$	$2\cdot3\cdot31$	$2^2\cdot59$	$2\cdot3\cdot43$	$2\cdot3^2\cdot17$	$2\cdot3^2\cdot53$	$2^2\cdot3^2\cdot37$	$2^2\cdot3\cdot31^2\cdot61$
$2\cdot13$	0	0	0	1	2	1	1	1	1	2	0	1	2	2	1	0
29	0	0	0	2	1	2	2	2	2	1	0	2	1	1	2	0
47	0	0	0	1	2	1	1	1	1	2	0	1	2	2	1	0
$2^2\cdot3\cdot5$	2	1	2	0	2	2	1	2	1	2	1	1	1	1	0	0
$3^2\cdot7$	1	2	1	1	0	2	0	2	0	0	2	0	1	1	1	0
$2\cdot3\cdot11$	2	1	2	1	1	0	2	0	2	1	1	2	0	0	1	0
$2\cdot41$	2	1	2	2	0	1	0	1	0	0	1	0	2	2	2	0
$2\cdot3\cdot23$	2	1	2	1	1	0	2	0	2	1	1	2	0	0	1	0
$3^2\cdot19$	2	1	2	2	0	1	0	1	0	0	1	0	2	2	2	0
$2\cdot3\cdot31$	1	2	1	1	0	2	0	2	0	0	2	0	1	1	1	0
$2^2\cdot59$	0	0	0	2	1	2	2	2	2	1	0	2	1	1	2	0
$2\cdot3\cdot43$	2	1	2	2	0	1	0	1	0	0	1	0	2	2	2	0
$2\cdot3^2\cdot17$	1	2	1	2	2	0	1	0	1	2	2	1	0	0	2	0
$2\cdot3^2\cdot53$	1	2	1	2	2	0	1	0	1	2	2	1	0	0	2	0
$2^2\cdot3^2\cdot37$	2	1	2	0	2	2	1	2	1	2	1	1	1	1	0	0
$2^2\cdot3\cdot31^2\cdot61$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

This is a rank 2 matrix, thus we see that the rank must be 13 and we have $Ш(\hat{E}/\mathbb{Q})[\hat{\phi}] \cong (\mathbb{Z}/3\mathbb{Z})^2$.

Example 6.1.4. Let

$$E : y^2 + xy = x^3 - 24515969818817808821988129496140681611 5x$$
$$+151019100990265579800255222064315889149061793786736008 8417$$

This curve is isomorphic to $E_{\varepsilon,\eta}$ where $\varepsilon = 25768271001$ and $\eta = -331337631523312128945489779 5200$. Then $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ is the subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^3$ generated by

$$\langle 3, 13, 2^2\cdot5, 2^2\cdot7, 2\cdot29, 2^2\cdot17, 3^1\cdot23, 2\cdot41, 2\cdot47, 2\cdot53, 2\cdot3\cdot19,$$
$$2^2\cdot43, 2\cdot89, 3\cdot11^2, 2^2\cdot3\cdot59, 2\cdot13\cdot31, 2\cdot13\cdot37, 13\cdot83\rangle$$

By Cassels' formula, $S^{(\phi)}(E/\mathbb{Q})$ is trivial. We have the number fields $L_1 = \mathbb{Q}(\zeta_3)$ and $M = \mathbb{Q}(\zeta_3, \beta)$ where

$$\beta^3 = 11\cdot29\cdot6099887\cdot1283387947\cdot585455194193$$

The torsion group $E[3]$ is generated by points S and T where

$$S = (0, -331337631523312128945489779 5200)$$
$$T = (-4\beta^2 - 34357694668\beta - 295112795724878907556,$$
$$\sqrt{-3}\,(-34357694668\beta^2 - 295112795724878907556\beta - 584822514726693259872550932 3052)).$$

Each generator of $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ has the following solution to the norm equation, up to cubes. Once again, the first four generators are sufficient to obtain the desired result, but we include the calculation for all generators for completeness' sake. Note that when we use the formula in Section 3.5.4, we must use $u = N_{M/L_1}(\xi)$.

Generator	ξ
3	$362923493385470815347368472435010433589060\beta^2$ $-20585741120452520430609264757575371135274068940295 56\beta$ $-272696964296306342060085648133303670140799759427993130232163 99$
13	$138584205218430608266267849231504786976322013961988 9\beta^2$ $+19704745887408522867063210766099735714258157003104077985910957 1\beta$ $-35267851604541194507811528778296557858890881851863279783901203900526788 74$
$2^2\cdot 5$	$941777368302148547380298026612930042865904655186515256236513 6\beta^2$ $+36360697423562359318071355720134949758705891479825824368160487259176950\beta$ $-16714116780178829570313591825670319762062908257147633227919017347976230000626220 74$
$2^2\cdot 7$	$-22253490672457559900047249187006197622130841309260804607394\beta^2$ $-15807705110844654883943964579780357208235326630096248601493061935785 2\beta$ $+49484952818786608293186895298884599000021725403144788040262359830238920473036 14$
$2\cdot 29$	$-68512730379250559574476289841918152527631993796070442066471954600\beta^2$ $+86829347242671125222252065160913973986109559556951870563637400892877 10697 85\beta$ $-87493710231984121829571968270920952065262551929745586080035334350544819653014530099 89$
$2^2\cdot 17$	$-10523144672321670374593796214928843545297305556213908523500\beta^2$ $+16148340807010272222316242885360919376690347809201612865601194389503 0\beta$ $-48526868087350313830359706383508144124285830480645203580220156278075779384260 6$
$3\cdot 23$	$140591288050181190979304591358290487983869 2\beta^2$ $-46704136175953074769777299088209938539981643303735 43\beta$ $-12906173271913789436719674161640621797200387463087604258044664 6$
$2\cdot 41$	$338986074204786065040023096026300881601419657376 5\beta^2$ $+51690672175640892649027915331978846574791763050203639484664\beta$ $+25802003074594317476274001540474650922536706555879588744938779001818 5$
$2\cdot 47$	$-91157143630434310947973605554258985797932935696741721578216636554540381022660 0\beta^2$ $-88211636233197731454882819895247019706056493144259948888459435186885343158017058809168 35\beta$ $+31790830114706016286355043229838055111234511333042603300486610050760826802689506779653411406822638 3$
$2\cdot 53$	$6343107817581986438062514472479981974187035570300886439 20\beta^2$ $+15033830480961099245253339561354399179342094101479447123279009533 9\beta$ $+39763920076774834461836823581658659395913526050783874933571710072113056223285$
$2\cdot 3\cdot 19$	$-37780398862807319272685318323030827470824767749479995965795201 97\beta^2$ $+29175013818957259849817974427989038632496046377595645269791564330830519320\beta$ $+16028892528044180950774668494086663489919413125993469394608144492322683074618854048 7$
$2^2\cdot 43$	$6397379759197730656560812426159189921558465086 62\beta^2$ $-17422061523868619776281256098028735115650963203307012426 84\beta$ $+21188515793827257623491597918178749072244038906788588146344571057770 2$
$2\cdot 89$	$-29271002319414247852135057298764766496445668427670023531635167615066823 6\beta^2$ $-61297621059494448125424391374849332791381586786951393577160028690628517000665888 0\beta$ $-68541079238729671506337480510313730978273278310681577146824646244077427217941961427452307348$
$3\cdot 11^2$	$-29960960640152098750491780433801030500528445743307422 60\beta^2$ $+27045041615990339253720335721636202888381124463896134925006980500\beta$ $+79198090627614006114362918227905595117440292149029582092120622267082314571$
$2^2\cdot 3\cdot 59$	$330848836159115954430971985246474318312963667357290939061033623840999289542375\beta^2$ $-13594784929645612237024129561438012639953015452871847201514249059486060012838413587733632\beta$ $+14327260374603139647925858953447603676141589450288149993649735169228140841623618708103100549578292 5$
$2\cdot 13\cdot 31$	$-19831517814143670150782754145789536767708937280400458445942278295 3\beta^2$ $-42386644704831832302306890081472670443993211406604285103625239233861627340 72\beta$ $+14231288479843395052711423818276480293534105508786721591110892023825216245180995065278 3$
$2\cdot 13\cdot 37$	$-47566501623948713296903108610035523035992178116331279225608758907062 37\beta^2$ $-46863120064437537480527048236628444125733861833609676360976383859722611227979584\beta$ $+13000929791901307580462412133895172879639301521684006204317284410409776676616948603111212 43$
$13\cdot 83$	$17785608032212618494113051928972773696912018233558424467889171519220\beta^2$ $+34558537804973132223262919177358135534321038855305721958586217083564927629117 5\beta$ $+12159714786264195783667687090978222094752005301564883914866929888724445250152490020696 98$

The set of bad primes over which we need to take the sum of local pairings is

$$P = \{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,83,89,6099887,1283387947,585455194193,$$
$$2144346275190060273 7,186118113519100907120218136235221960204803459121299833503713\}.$$

We obtain the following 18×18 matrix for the Cassels-Tate pairing.

	3	13	$2^2\cdot5$	$2^2\cdot7$	$2\cdot29$	$2^2\cdot17$	$3^1\cdot23$	$2\cdot41$	$2\cdot47$	$2\cdot53$	$2\cdot3\cdot19$	$2^2\cdot43$	$2\cdot89$	$3\cdot11^2$	$2^2\cdot3\cdot59$	$2\cdot13\cdot31$	$2\cdot13\cdot37$	$13\cdot83$
3	0	1	1	2	0	1	2	0	1	0	2	2	2	1	2	2	2	1
13	2	0	2	0	2	2	0	1	0	0	0	2	0	1	0	0	2	2
$2^2\cdot5$	2	1	0	0	2	1	1	2	0	1	2	1	2	1	1	0	2	2
$2^2\cdot7$	1	0	0	0	0	2	0	0	1	0	2	1	1	2	2	2	0	1
$2\cdot29$	0	1	1	0	0	2	1	1	0	1	2	2	2	0	1	0	0	0
$2^2\cdot17$	2	1	2	1	1	0	0	1	0	2	1	1	0	0	2	0	2	1
$3^1\cdot23$	1	0	2	0	2	0	0	1	2	0	1	1	2	2	1	1	2	1
$2\cdot41$	0	2	1	0	2	2	2	0	1	2	0	1	2	0	1	2	2	0
$2\cdot47$	2	0	0	2	0	0	1	2	0	2	1	2	2	2	2	0	2	0
$2\cdot53$	0	0	2	0	2	1	0	1	1	0	2	0	1	0	2	2	2	0
$2\cdot3\cdot19$	1	0	1	1	1	2	2	0	2	1	0	1	0	1	2	1	2	0
$2^2\cdot43$	1	1	2	2	1	2	2	2	1	0	2	0	2	0	2	2	0	2
$2\cdot89$	1	0	1	2	1	0	1	1	1	2	0	1	0	0	1	2	0	2
$3\cdot11^2$	2	2	2	1	0	0	1	0	1	0	2	0	0	0	2	2	1	1
$2^2\cdot3\cdot59$	1	0	2	1	2	1	2	2	1	1	1	1	2	1	0	2	0	0
$2\cdot13\cdot31$	1	0	0	1	0	0	2	1	0	1	2	1	1	1	1	0	1	0
$2\cdot13\cdot37$	1	1	1	0	0	1	1	1	1	1	1	0	0	2	0	2	0	1
$13\cdot83$	2	1	1	2	0	2	2	0	0	0	0	1	1	2	0	0	2	0

This is a rank 4 matrix, thus we obtain an upper bound of 13 on the rank and we have $Ш(\hat{E}/\mathbb{Q})[\hat{\phi}] \cong (\mathbb{Z}/3\mathbb{Z})^4$. The rank must therefore be precisely 13.

Thus far no elliptic curve with torsion subgroup over $\mathbb{Q}$ equal to $\mathbb{Z}/3\mathbb{Z}$ has been found with rank larger than 13.

6.2 Torsion Group $\mathbb{Z}/9\mathbb{Z}$ Over $\mathbb{Q}$

In this section, we look for high rank curves in the family of elliptic curves with $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$. Each such a curve can be written in the form $E_9(s,t)$, as in Proposition 6.0.2, with $P = (0,0)$ a point of order 9. The class of isogenous curves has 3 members in each case. We let ϕ_1 be the 3-isogeny with kernel $\{O, 3P, 6P\}$ and obtain the following diagram of curves with torsion groups.

$$\begin{array}{ccccccccc} \mathbb{Z}/9\mathbb{Z} & & \mu_3 \times \mathbb{Z}/3\mathbb{Z} & & \mu_9 & & \mu_3 \times \mathbb{Z}/3\mathbb{Z} & & \mathbb{Z}/9\mathbb{Z} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ E & \xrightarrow{\phi_1} & E' & \xrightarrow{\phi_2} & E'' & \xrightarrow{\hat{\phi}_2} & E' & \xrightarrow{\hat{\phi}_1} & E \end{array}$$

To estimate the rank, we can use either the pair of isogenies $\phi_1, \hat{\phi}_1$ or alternatively the pair $\phi_2, \hat{\phi}_2$. Using Section 2.6 we use ϕ_1 and $\hat{\phi}_1$ to calculate the Selmer groups $S^{(\phi_1)}(E/\mathbb{Q})$ and $S^{(\hat{\phi}_1)}(E'/\mathbb{Q})$. In [Fis03] we see how to compute the Cassels-Tate pairing on $S^{(\phi_1)}(E/\mathbb{Q})$ and so we are left with the task of computing

the pairing on $S^{(\hat{\phi}_1)}(E'/\mathbb{Q})$. We can then estimate the rank using the formulae given in Section 2.7. Using the pair of isogenies ϕ_2 and $\hat{\phi}_2$ would also give a useful rank estimate, however we choose not to pursue this any further here as we prefer to work with the curve having split torsion.

The following example gives the flavour of all the calculations done in this section and demonstrates how this method has been useful to us.

Example 6.2.1. Let $s = -11$ and $t = 28$, and consider the curve

$$E_9(-11,28) : y^2 + 26671xy + 3518381298432y = x^3 + 160276116x^2.$$

We obtain the Selmer group $S^{(\hat{\phi}_1)}(E'/\mathbb{Q}) = \langle 12, 13, 22, 28\rangle$ as a subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^3$. By Cassels' formula (6.1) we find that $S^{(\phi_1)}(E/\mathbb{Q})$ is generated by one element. Thus the upper bound for the rank is 4. To use the formula in Section 3.5.4 we need the following data. We have $\varepsilon = 31371$ and $\eta = 187184432058624$. We have $L = \mathbb{Q}(\sqrt{-3})$ and $M = L(\beta)$ where $\beta^3 = 25579$. The norm equations $N_{M/L}(\xi) = g$ are solved by the following elements.

g	ξ
12	$\frac{1}{7812}\left(-5\beta^2 - 47\beta + 18307\right)$
13	$\frac{1}{46162627}\left(89539\beta^2 + 2264810\beta + 138749830\right)$
22	$\frac{1}{27867174}\left(46165\beta^2 + 3166919\beta + 42616353\right)$
28	$\frac{1}{15}\left(\beta + 41\right)$

The set of bad primes of E is $P = \{2, 3, 7, 11, 13, 1213, 25579\}$ and in this case we need not expand this set. By finding a local point on the covering curves for each p in P and using Definition 3.3.2 we obtain the following matrix for the Cassels-Tate pairing on $S^{(\hat{\phi}_1)}(E'/\mathbb{Q})$.

	12	13	22	28
12	0	0	2	1
13	0	0	0	0
22	1	0	0	2
28	2	0	1	0

This matrix has rank 2, therefore the new upper bound on the rank is 2. In fact, we can find two independent points on E, therefore its rank is exactly 2.

$$P_1 = \left(-\frac{97599598156093313 28}{88534217209}, -\frac{29524080122808992201584591488}{26343090727886323}\right)$$

$$P_2 = \left(\frac{358129710275997660}{12752041}, -\frac{23274616826719887242533 9200}{45537538411}\right)$$

We have also found that $Ш(\hat{E}/\mathbb{Q})[\hat{\phi}] \cong (\mathbb{Z}/3\mathbb{Z})^2$.

The following example is given to demonstrate how the method is also practical in large examples. Also, this is a rather special curve under consideration.

Example 6.2.2. Let $s = -23$ and $t = 385$, and consider the curve

$$E_9(-23,385) : y^2 + 57282457xy + 747377065518723255000y = x^3 + 13096570289880x^2$$

We obtain the Selmer group $S^{(\hat{\phi}_1)}(E'/\mathbb{Q}) = \langle 17, 2\cdot 3\cdot 5, 3^2\cdot 7, 3^2\cdot 11, 5\cdot 23\rangle$ as a subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^3$. By Cassels' formula (6.1) we find that $S^{(\phi_1)}(E/\mathbb{Q})$ is trivial, thus the upper bound on the rank is 4. To use the formula in Section 3.5.4 we need the following data. We have $\varepsilon = 169330389$ and $\eta = 5092956201458264832000$. We have $L = \mathbb{Q}(\sqrt{-3})$ and $M = \mathbb{Q}(\sqrt{-3}, \beta)$ where $\beta^3 = 251\cdot 181693$. The norm equations $N_{M/L}(\xi) = g$ are solved by the following elements. Once again, for ease of presentation the norm of the element ξ is only the same as the generator up to powers of 3. To use the formulae in Section 3.5, we must use the exact norm of ξ.

g	ξ
17	$60307829666942700\beta^2 - 209302881620322855420\beta - 101177927393421172079417$
$2\cdot 3\cdot 5$	$-136846042944\beta^2 + 193121610684468\beta - 230748564240645900$
$3^2\cdot 7$	$212106325495260\beta^2 + 29628816651061472\beta + 12569924072032381379$
$3^2\cdot 11$	$-16944109161772878289669525002 7\beta^2 - 60930323308035375847595809084 36\beta$ $+26042983014981080970503823422800902$
$5\cdot 23$	$28538901754848336\beta^2 - 26496624672381328 9745\beta + 98197755254050027074236$

The set of bad primes of E is $P = \{2,3,5,7,11,17,23,251,397,181693\}$. Unfortunately, in this case we obtain an incorrect answer if we simply continue the calculation from this point onwards using only these primes. We must extend this set to include other primes introduced by our choice of pushout forms, as described in Proposition 3.3.6, giving us

$$P = \{2,3,5,7,11,17,23,37,251,397,523,19501,44587,181693,391999,4978335031,576681614287,$$
$$2512745948431,70237237108447,11065466550444247,6536123176275678832447\}.$$

We now have all the tools we need to use Definition 3.3.2. We obtain the following matrix for the Cassels-Tate pairing on $S^{(\hat{\phi}_1)}(E'/\mathbb{Q})$.

	17	$2\cdot 3\cdot 5$	$3^2\cdot 7$	$3^2\cdot 11$	$5\cdot 23$
17	0	0	0	0	0
$2\cdot 3\cdot 5$	0	0	0	0	0
$3^2\cdot 7$	0	0	0	0	0
$3^2\cdot 11$	0	0	0	0	0
$5\cdot 23$	0	0	0	0	0

Thus the upper bound on the rank remains 4. In fact, this is the first curve found with torsion subgroup $\mathbb{Z}/9\mathbb{Z}$ over $\mathbb{Q}$ and rank 4, discovered in 2009 by T. Fisher [Duj15]. No higher rank curve has yet been found in this family.

We used these calculations to find other curves of rank 4 or higher in this family. We searched through all s,t with $|s| \leq 1600$ and $|t| \leq 2000$. The following table lists a representative sample of the results

of our calculations. By this we mean that all curves having potentially high rank are included, with a number of other curves selected at random with a fairly even spread over the two parameters. The first two columns give the values for s and t, and N denotes the conductor of the resulting curve. The column denoted by r_{ϕ_1} denotes the rank upper bound after calculating a descent by 3-isogeny using ϕ_1. We denote by ϕ_1 and $\hat{\phi}_1$ the number of generators of the Selmer groups $S^{(\phi_1)}(E/\mathbb{Q})$ and $S^{(\hat{\phi}_1)}(E'/\mathbb{Q})$, respectively. $\mathrm{Rank}(\hat{M})$ denotes the rank of the matrix $\hat{M}$ representing the Cassels-Tate pairing on $S^{(\hat{\phi}_1)}(E/\mathbb{Q})$. Finally, the column r denotes the new rank upper bound in light of the pairing computed.

In order to limit our search space, we applied other rank estimates to discard low rank curves, namely the following. In Section 2.6, we discussed the Cassels-Tate pairing in cases where an elliptic curve E has split torsion. We used all three rank estimates from Theorem 2.6.4. We also calculated a 2-descent, and occasionally lifted this to a 4-descent using the Cassels-Tate pairing implemented in MAGMA.

s	t	N	r_{ϕ_1}	$\hat{\phi}_1$	ϕ_1	$\mathrm{Rank}(\hat{M})$	r
5	1491	82171094696824089302430	4	5	0	2	2
8	1253	9756129801739187586090	4	5	0	4	0
−10	627	53411588599801021590	4	5	0	4	0
11	203	5017832262458862	4	4	1	2	2
11	1896	243539568404512801831410	4	5	0	2	2
−12	1919	571187810496560520655218	4	4	1	2	2
−15	481	10705857838425842430	4	5	0	4	0
−23	385	16352763705110910	4	5	0	0	4
33	140	15114894561669210	5	5	1	2	3
−55	524	227270128080889966710	4	4	1	2	2
−57	151	27802374961524618	4	3	2	2	2
89	287	3569021367011884938	5	5	1	2	3
−118	545	152917324959907271010	4	5	0	4	0
119	485	641880765166790453010	4	5	0	2	2
131	555	461368665311312172930	4	5	0	4	0
133	507	72964018791848021838	4	5	0	2	2
144	529	2457177494631050730	4	5	0	4	0
−144	683	57803171579013534834	4	4	1	2	2
145	681	2220448668365578567530	4	4	1	2	2
152	411	48732371824822036386	4	5	0	2	2
161	327	27987122665913236014	4	4	1	2	2
−163	369	94487214034344749394	4	4	1	2	2
172	471	289859532170344821282	4	5	0	2	2
−172	969	26797305084314477127198	5	5	1	4	1
−174	541	144770615593899871290	4	4	1	2	2
−179	255	206646839618507357370	4	5	0	2	2
−183	622	5035192634461546011210	4	5	0	2	2
−240	473	9290231278866356718 90	4	4	1	0	4
−255	1426	28308537820366840699530	4	5	0	4	0
255	1817	164561968489049160893567 90	6	7	0	6	0
257	1853	95278358733110927767008 42	5	6	0	4	1
−259	1509	492352366052547256755954	4	5	0	2	2
259	1705	10586305470575663938962930	4	5	0	2	2
−341	702	16185091251318922858926	5	6	0	4	1
−341	721	53709329454870901899318	5	6	0	4	1

s	t	N	r_{ϕ_1}	$\hat{\phi}_1$	ϕ_1	$\mathrm{Rank}(\hat{M})$	r
-341	754	190572315887243764157970	4	5	0	2	2
-345	913	399200781246220004260110	6	7	0	6	0
-345	979	251214046236894607213710	4	5	0	4	0
-355	629	28352480766588873916770	4	4	1	0	4
-421	399	22111533813260234570010	4	5	0	4	0
-437	660	162592535727253391183490	4	5	0	2	2
-457	392	2168698111927772329758	4	4	1	2	2
-555	1162	76450779993759613144859l0	4	5	0	4	0
559	1345	25252089175154818962152 70	6	6	1	4	2
-585	1418	66793675593890584199363l0	4	5	0	2	2
587	1182	809077366944910527046590	4	5	0	4	0
-595	1184	687649370057565185702670	4	5	0	4	0
629	1974	54043940442916338535336170	4	5	0	4	0
-630	1063	30847741273672839584256 30	6	6	1	4	2
-638	1915	81489049512976120267151130	4	5	0	4	0
-639	1022	28169536123557116997365 58	5	6	0	4	1
-644	1461	16963206149574239751359310	4	5	0	4	0
644	1805	78760665630533682116790	5	6	0	4	1
-663	1880	23310839010161074083921690	5	6	0	4	1
683	1961	17385765324353996728527678	5	5	1	4	1
697	1690	12093981413838724354847l0	4	5	0	4	0
-700	1181	716353050035024366720910	4	5	0	2	2
-701	1144	1595354034708705174485010	4	5	0	2	2
701	1790	762070172755765990085970	4	4	1	2	2
-702	1241	2920785200397549650442966	4	4	1	2	2
-703	1040	1685809875827673115411710	4	5	0	2	2
-703	1268	1595202222569601651313398	4	5	0	2	2
-703	1442	46882286995338869626141590	6	7	0	6	0
703	1618	10906162045465041924718170	4	5	0	4	0
-704	1665	839837364157852965493710	4	5	0	4	0
-739	572	1011273903693573949648362	4	5	0	4	0
-751	978	61931907898002777218766	4	5	0	2	2
-786	559	25252089175154818962152 70	6	6	1	4	2
-807	770	82505987019238444360799l0	4	5	0	2	2
-811	555	28745606054334159531462 30	4	5	0	2	2
-817	845	92826563851450464306297 0	4	5	0	4	0
-819	626	86643853774805978417130	4	5	0	4	0
-849	784	197552370463860808523694	4	5	0	4	0
-867	659	4026276224217606856052 22	4	5	0	2	2
-870	929	22342307875162186036265070	4	5	0	4	0
-873	436	3402373427883318953881 74	4	5	0	4	0
-986	849	28881156563973328674974010	4	5	0	2	2
-993	697	12093981413838724354847l0	4	5	0	4	0
-995	153	3502917135023206338690	4	5	0	2	2
-999	650	289643337657958864373430	4	5	0	2	2
-1000	807	260617313114559955110570	4	5	0	4	0
-1012	1137	44921480364568313275234542	4	5	0	2	2
-1021	1589	10785993268033806037416537 0	4	5	0	4	0

s	t	N	r_{ϕ_1}	$\hat{\phi}_1$	ϕ_1	Rank$(\hat{M})$	r
-1040	1453	10391473408732119746385330	4	5	0	4	0
-1051	1035	25399371345088353798573570	4	4	1	0	4
-1079	1998	10864686704340434322675138 6	4	5	0	2	2
-1085	1006	79813751502622016753117790	4	5	0	2	2
-1091	1738	60106165993130941462275677 4	4	5	0	4	0

Using this method, we were successful in finding two new curves in this family of rank 4. They are listed in the table below, in the format s,t, where the curve is formed by using Proposition 6.0.2. In Chapter 7 we will explore further ways of eliminating curves that do not have a high rank. We were unable to find more than 2 generators for $E_9(-1051,1035)$, but neither have we been able to rule out that it has rank 4, therefore we shall revisit it in Chapter 7.

s	t	independent points
-240	473	$\left(-\frac{383531650410344842560}{96721}, -\frac{1148428608086443239325858223520 0}{30080231}\right)$ $\left(\frac{817244603698770247952829720192799680 00}{6049592989355610207529}, \frac{477285525211729143108026474745450251945877199678464000000}{4705320766805227666380990007786 67}\right)$ $\left(-\frac{543902678599722229553137998912 00}{9719666896433641}, \frac{249208504105729270874004955488343663486033920000}{9582461259820183757888 11}\right)$ $\left(-\frac{131860026844068289709447 68}{4437291769}, \frac{264024786102425482534495759868488130 56}{295581316608397}\right)$
-355	629	$\left(\frac{869286662994967611141554714418 00}{94700982862249}, -\frac{101613013420942351369581758723367766254132811 6800}{921577216767952995307}\right)$ $\left(\frac{50154140332101652680}{7921}, -\frac{119659848118677077122867000176 00}{704969}\right)$ $\left(-\frac{364794282942887665425166625400}{6743936354281}, \frac{128108078825455684973562231057142189856040000}{17513389013859517429}\right)$ $\left(\frac{737344898757333287275683534258 00}{184337834489449}, \frac{503100254051627822311222612736592092090302680000}{2502774503011539444043}\right)$

6.3 Torsion Group $\mathbb{Z}/12\mathbb{Z}$ Over $\mathbb{Q}$

We now investigate the family of curves with torsion group $\mathbb{Z}/12\mathbb{Z}$. Proposition 6.0.3 gives a parametrisation for such curves, with $P=(0,0)$ a point of order 12. There are 8 curves in the isogeny class of such a curve E. We let ϕ be the 3-isogeny with kernel $\{O,4P,8P\}$ and obtain the following diagram.

$$\begin{array}{ccccc} \mathbb{Z}/12\mathbb{Z} & & \mu_3\times\mathbb{Z}/4\mathbb{Z} & & \mathbb{Z}/12\mathbb{Z} \\ \downarrow & & \downarrow & & \downarrow \\ E & \xrightarrow{\phi} & \hat{E} & \xrightarrow{\hat{\phi}} & E \end{array}$$

Once again, we calculate the Selmer groups $S^{(\phi)}(E/\mathbb{Q})$ and $S^{(\hat{\phi})}(E'/\mathbb{Q})$ using [Fis03] and then calculate the Cassels-Tate pairing. The following example gives a full calculation of the Cassels-Tate pairing on $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$.

Example 6.3.1. Let $s=-10$ and $t=13$, and consider the curve

$$E_{12}(-10,13): y^2-54701xy-9579281428470y=x^3+189572370x^2$$

We obtain the Selmer group $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})=\langle 6,10,39,807\rangle$ as a subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^3$. By Cassels' formula (6.1) we find that $S^{(\phi)}(E/\mathbb{Q})$ is trivial. Thus the upper bound for the rank is 3. To use the formula

in Section 3.5.4 we need the following data. We have $\varepsilon = 94137$ and $\eta = -74677875480000$. We have $L = \mathbb{Q}(\sqrt{-3})$ and $M = \mathbb{Q}(\beta)$ where $\beta^3 = 23^2 \cdot 139 \cdot 251$. The norm equations are solved by the following elements. Once again, the generator is only accurate up to cubes. We need to use the actual norm of each element ξ in the formula.

Generator	ξ
6	$-10362501547963233399 12\beta^2 - 10721215099393110475552 5\beta$ $+10313848838325591008030021 1$
10	$1356521163\beta^2 - 2369174660160\beta + 812363652771427$
39	$17641089431102400\beta^2 - 3294528492339431025\beta - 199128822887169881 3118$
807	$3225776740053120655571343253638390146879518886232\beta^2$ $-4128279026812805304178610976142603373120740495 0725\beta$ $-2264693391916886097519412180852632373418073032624512 86$

The set of bad primes of E is $P = \{2,3,5,13,23,139,251,269\}$, which we expand as is explained in Proposition 3.3.6 to

$$P = \{2,3,5,13,23,61,67,73,139,251,269,457,419161,2170141,4999781257,665374861243,$$
$$4820055638617,153827896655203,421605961152165175507327122 1\}.$$

By finding a local point on the covering curves for each p in P and using Definition 3.3.2 we obtain the following matrix.

	6	10	39	807
6	0	2	0	1
10	1	0	0	0
39	0	0	0	0
807	2	0	0	0

This matrix has rank 2, therefore the new upper bound on the rank is 1. A generator is not known on this curve. We have also found that $Ш(\hat{E}/\mathbb{Q})[\hat{\phi}] \cong (\mathbb{Z}/3\mathbb{Z})^2$.

Once again, we attempted to use these calculations to find other curves of rank 4 or higher in this family. To eliminate unsuitable curves, we could employ stronger machinery than in the previous family, by exploiting the fact that any elliptic curve E with torsion group $\mathbb{Z}/12\mathbb{Z}$ has a rational point of order 2. Thus we could calculate a 2-isogeny descent, and use the theory from Section 2.7 to obtain ever more accurate bounds on the rank of E. This procedure is implemented in version 21 of MAGMA by T. Fisher, as `TwoPowerIsogenyDescentRankBound`. We searched through all $|s|,|t| \leq 7500$ to find rank 4 candidates, and all $|s|,|t| \leq 13500$ for rank 5 candidates. (Note: we had to exclude the pairs $(s,t) \in \{(-6157,5486),(-6263,4264),(6397,5556),(7387,2008)\}$ as the calculation in these cases involved primes that were too large to perform the computation, even on a part of the Selmer group. All of these are candidates for rank 4.)

The following table lists many examples, a full list would be somewhat too cumbersome so we have selected a representative sample. We have selected all interesting examples which still have potentially

high rank, together with a number of other curves selected at random from the sample set. We did not include any of the examples on which we calculated the pairing on only a subset of the Selmer group to save on the number of computations to be performed. We give the values for s and t in the first two columns. N denotes the conductor of the curve. The column denoted r_ϕ gives the upper bound on the rank after computing a descent by 3-isogeny. We denote by ϕ and $\hat{\phi}$ the number of generators of the Selmer groups $S^{(\phi)}(E/\mathbb{Q})$ and $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ respectively. $\mathrm{Rank}(\hat{M})$ is the rank of the matrix $\hat{M}$ representing the pairing on $S^{(\hat{\phi})}(E/\mathbb{Q})$. Finally, the last column r denotes the new rank estimate in light of the pairing computed.

s	t	N	r_ϕ	$\hat{\phi}$	ϕ	$\mathrm{Rank}(\hat{M})$	r
-408	337	137003109467305395552810	4	5	0	2	2
-584	329	41250114769296437283662290	6	7	0	4	2
-623	552	23677250941983513617743 7490	6	7	0	4	2
684	155	91852854210635848198432590	6	7	0	4	2
859	593	35821052991524475959164881 0	4	5	0	0	4
-891	650	13586970645162682512709064 10	4	5	0	4	0
-985	433	48423398781034346986153686 90	4	5	0	4	0
1081	912	11335916522820254830031414913 0	6	7	0	4	2
1128	481	15964007771985921244450646180 70	4	5	0	4	0
1169	552	28202203146272683019823313628 10	4	5	0	4	0
-1225	444	94806918255675408725273030 70	6	7	0	6	0
1321	270	85000661913531219425752428093 0	4	5	0	4	0
-1343	1320	60510166019239493564075549481 0	4	5	0	4	0
-1369	1170	12278647132204848102012330987 0	4	4	1	2	2
1391	924	62590535508748698422683937034810	8	9	0	8	0
1443	670	89458825285606816224354050867310	6	7	0	6	0
1443	1078	30144000376281971242314452971770	4	5	0	2	2
1568	1089	12013792511915234042171655717 0	6	7	0	6	0
1585	72	46970874810962632124381130639 0	4	5	0	4	0
1639	260	72621318691084638720428522238 90	4	5	0	4	0
1705	156	14355633727189357808694771191910	4	5	0	4	0
1755	1198	14840040207638313187441202087859 0	4	5	0	4	0
-1780	357	63878781661697458894658989927 0	6	7	0	6	0
1780	1539	30671687802918342018360580083870	6	7	0	4	2
1830	553	40457122367310409855869228583311 0	4	5	0	4	0
1845	1036	25747810887013522870536117246333 0	6	7	0	6	0
-1876	93	20509737532634161372941394221 90	4	5	0	4	0
1885	1698	25593037626047100663113242942058 70	6	7	0	6	0
1916	1533	18595021304839624265919636427826 10	6	7	0	4	2
-1957	828	21825260860501579301856305774790	6	7	0	6	0
2038	1547	67511327967667244448378450745512 90	6	7	0	6	0
2068	1751	15405500434565195209653468113901 0	6	7	0	6	0
-2072	143	17158617479601255343182555368310	6	7	0	6	0
2113	2070	79031552286317741959391544356187 0	4	5	0	2	2
2196	515	27699268736580822598267490973 0	6	7	0	4	2
2209	399	35338827732665790261786782001 0	6	7	0	6	0
-2262	2255	85618749613899696962209387935990	8	9	0	8	0
-2297	1649	26985299387803029893258475825 90	4	5	0	4	0
2328	1075	52819768104027269022095813629143 0	4	5	0	4	0

s	t	N	r_ϕ	$\hat{\phi}$	ϕ	Rank$(\hat{M})$	r
2356	213	358416901938552100761283435638390	4	5	0	2	2
2362	1349	188975064633444893490577194843867 30	6	7	0	4	2
−2495	972	68051620158548404884918833546 70	4	5	0	4	0
−2598	1901	81769062788273023531365352451 1130	4	5	0	2	2
−2616	2159	46036479766345093500220127803 2090	4	5	0	4	0
−2644	951	70299095900020338501439169532 9630	4	5	0	4	0
−2647	595	32869300031559608034873402047 10	4	5	0	4	0
−2651	1325	28222347704325960119817765112230	4	5	0	4	0
2668	369	69669394778212529777035757324610	4	5	0	2	2
2712	1129	89121285343042795723988427245 2110	4	5	0	4	0
2721	140	72906015271443792799236064092 2670	4	5	0	4	0
−2751	316	64466329396459941189932177425710	4	5	0	2	2
−2753	2552	26128569661313784955882161513467 70	4	5	0	4	0
−2756	825	63939680935990238153815467471330	4	5	0	2	2
−2766	655	55187334721740166694044249506 3330	4	5	0	4	0
2796	1795	63612222490513330088382538632531510	4	4	1	2	2
−2840	591	31222645501522353069309018221 9190	6	7	0	6	0
2852	1215	59999215815004570225145869896870	4	5	0	4	0
2913	416	29067885742000009070989149228330	4	5	0	4	0
2927	2385	33417264489812100150086140514 2590	4	5	0	4	0
2928	2869	76675083616292365191534940857792 90	6	7	0	6	0
3020	309	50999311045550469542465003275676 10	4	5	0	4	0
3077	1506	19403607931382378890230843118539 2190	4	5	0	4	0
−3087	2990	11654060565054023416849882669 7910	4	5	0	4	0
3097	1872	37718540681483401069936669304 2410	6	6	1	2	4
3128	2779	21485963046684304713102924569772030	8	9	0	6	2
3129	88	72453452240289556533233964763 5510	4	5	0	4	0
3133	3117	81854523155657291412370292 8410	4	5	0	4	0
3169	3143	18171417922059568181457304440 09570	4	5	0	4	0
−3192	2129	13972354663113459262849690770881070	4	5	0	2	2
3213	404	26785939357151069961798765850290	4	5	0	4	0
3219	169	70158310187158403474345542 4610	4	5	0	2	2
3241	1992	12875179318761733037073673135559 1570	4	5	0	4	0
3265	2076	42124335463203449196454192840886490	4	5	0	2	2
3276	2789	12673525195631458680200467212895 1070	4	5	0	2	2
−3282	2291	79494088012395687208190459341499970	4	5	0	2	2
3299	708	39255771813904796472265394172889230	4	5	0	4	0
3319	2280	19726033711002529084735088519943 3030	6	7	0	6	0
−3342	2353	96492839556597889777604879031733530	6	7	0	6	0
−3344	1281	74217464059936375028066241725 70	4	5	0	4	0
−3400	517	18287563996620119932732694694210	6	7	0	6	0
−3429	2210	11935209850919341197788509794088890	6	7	0	4	2
3431	840	36681336645401795723607379477784910	6	7	0	6	0
−3439	1533	27243427141440110847617014186643 10	6	7	0	4	2
−3459	2242	11846049901653758287320149365986 8430	6	7	0	4	2
3470	429	53794113657317052247085959337306070	6	7	0	6	0
−3535	1683	14584153662038315469251269404680 10	6	7	0	6	0
3552	1765	52586455095136617765713719228010730	4	5	0	4	0

s	t	N	r_ϕ	$\hat{\phi}$	ϕ	$\mathrm{Rank}(\hat{M})$	r
3553	3023	267789972415893732428257434183368 70	6	7	0	4	2
3584	3289	554574688021728198544147692285021 0	6	7	0	6	0
3603	2258	153882894749100842429109691319099937 0	4	5	0	4	0
3623	481	319917757343874277535816006858070	6	7	0	6	0
−3636	3485	185145736983147742955553376002717 90	4	5	0	4	0
−3654	767	505294464495680553648233015314851 0	6	7	0	6	0
−3687	3070	404101443834507041402506530941892 30	4	5	0	2	2
−3695	59	145451116591661273882092803260490	4	5	0	2	2
−3755	1716	115696767193349597293863997213041 0	4	5	0	4	0
3773	3306	598303312602408983593707017162343 90	6	7	0	6	0
−3828	1025	95781368908537026832298348310	4	5	0	2	2
−3836	1373	436847231079146626851335095943070	4	5	0	4	0
3839	2545	499847570148914244145617025745147 70	8	9	0	8	0
3933	2420	541517658482528450855376713331116 10	4	5	0	4	0
−3939	236	168861892303727651296048672434270	6	7	0	6	0
3940	2307	165502388680954766913470383869087021 0	4	5	0	4	0
3959	3234	115486144571473549400667209514545 10	4	5	0	2	2
−3960	3031	370006117027631375684500623326811 0	4	5	0	4	0
−3964	1855	349926603899249835850600146848910	6	7	0	4	2
−3985	2328	982153437223878044789722518951329 70	4	5	0	2	2
3999	442	269627893808919651597480450202340 70	6	7	0	6	0
−4039	4015	167103642433009400023028016512157 0	4	5	0	4	0
4052	1221	569892536794977433725443674374088 710	4	5	0	2	2
−4057	1170	645162306081381090945751375499127 0	4	5	0	4	0
4095	3064	596490600715976529903449477835904 710	6	7	0	4	2
−4115	2484	323477893977177630255408333780017 70	6	7	0	6	0
4121	3544	185256005099992410809477535610855 9830	4	5	0	2	2
4370	3597	140557044911149836349494663525953582 10	8	9	0	6	2
4602	2965	186795687579039198571389299511775203 30	8	9	0	6	2
4833	1720	255702732290262639821720443387535 310	4	4	1	2	2
4896	155	607840184174455244802588632982291 0	5	6	0	4	1
−5219	1008	538528051549371672402219555852903 0	8	8	1	6	2
5676	2653	402129258647981818425214717653097719 30	8	9	0	6	2
5693	4866	271054708233400323339059967020754302 10	4	4	1	2	2
−5871	2240	165104209003954024251482713192225830	8	9	0	6	2
−5950	1537	407110869250756922288355101817873 0	6	7	0	4	2
5957	744	303537661977083637425443448911965381 0	6	7	0	6	0
5972	931	533029235404692957067176755726010	8	9	0	6	2
6521	1540	422984604623117492844939019390023533 70	8	9	0	6	2
6585	3052	174527423105334360489438184862185578990	6	7	0	6	0
6648	5159	233362592076506418782186442347476846590	5	6	0	4	1
−7189	1452	132035766093222249764437035325911690	6	6	1	2	4
−7359	3376	119849101005187956601286440744942343 10	4	5	0	4	0
8525	7842	161895028727938388473293386791924472799 0	5	6	0	4	1

There are several curves of interest in this table. The first is $E_{12}(859,593)$, which is the only known curve of rank 4 in this family, discovered by T. Fisher in 2008 [Duj15]. There are no known curves of higher rank at the date of writing. The other curves of interest are $E_{12}(3097,1872)$ and $E_{12}(-7189,1452)$, which

are the only survivors in this procedure and therefore the only curves so far worth investigating further. We will investigate a strategy for doing this in Chapter 7, although these curves will prove to have too large coefficients to be handled there. Note also Example 7.2.2, which handles a single case separately, for reasons explained in that example.

Chapter 7

Further Descent Calculations in the 3-Isogeny Case

In the previous chapter, we searched for high rank curves in certain families. We had a few examples which were candidates for high rank curves but we could not find generators for the Mordell-Weil group to prove the upper bound was actually attained. In this chapter, we will use the strategy from Section 3.6 to give a more accurate upper bound on the rank.

7.1 The Method

Let n be any integer and let E be an elliptic curve admitting a cyclic n-isogeny

$$\phi : E \longrightarrow \hat{E}$$

with $\hat{\phi} : \hat{E} \to E$ be its dual. Let $E[n]$ be generated by S and T such that $E[\phi] = \langle S \rangle$. Let $S^{(\phi)}(E/K)$ and $S^{(\hat{\phi})}(\hat{E}/K)$ denote the Selmer groups attached to ϕ and $\hat{\phi}$ respectively. In Section 3.1, we saw that the kernel of the Cassels-Tate pairing on $S^{(\hat{\phi})}(\hat{E}/K) \times S^{(\hat{\phi})}(\hat{E}/K)$ is the image of $S^{(n)}(E/K)$. Thus we could turn a descent by n-isogeny into a full n-descent.

In this chapter, we will be computing the Cassels-Tate pairing

$$S^{(\phi)}(E/K) \times S^{(n)}(E/K) \longrightarrow \mathbb{Q}/\mathbb{Z} \tag{7.1}$$

whose right kernel is precisely the image of the Selmer group $S^{(n\phi)}(E/K)$. We will use the pushout function definition of the pairing, namely Definition 3.3.2.

7.1.1 Preliminary Theory

In Sections 2.2 and 2.3, we saw that elements of $S^{(n)}(E/K)$ could be written both as elements of some concrete group and as n-coverings of E. In this chapter, we need another geometric interpretation of the cohomology group $H^1(K, E[n])$, in which this Selmer group lies. The following terminology comes from [CFO+08].

Definition 7.1.1. A *torsor divisor class pair* $(C, [A])$ is a torsor C under E together with a K-rational divisor class $[A]$ on C of degree n.

The divisor A is linearly equivalent, but not necessarily equal, to its Galois conjugates. The isomorphism of torsor divisor class pairs $(C_1,[A_1]) \cong (C_2,[A_2])$ is an isomorphism $\psi : C_1 \cong C_2$ such that $\psi^* A_2 \sim A_1$. The trivial torsor divisor class pair is $(E,[n\cdot\mathscr{O}])$, and every torsor divisor class pair is a twist of this. The torsor divisor class pairs are parametrised up to isomorphism by $H^1(K,\mathrm{Aut}(E,[n\cdot\mathscr{O}]))$. For consider any $(C,[A])$ with

$$\psi : (C,[A]) \longrightarrow (E,[n\cdot\mathscr{O}])$$

an isomorphism defined over $\bar{K}$. Then we associate to $(C,[A])$ the cocycle $\xi_\sigma = \sigma(\psi)\psi^{-1}$. The following lemma completes the characterisation of $H^1(K,E[n])$ as torsor divisor class pairs.

Lemma 7.1.2 ([CFO+08, 1.8])**.** *$Aut(E,[n\cdot\mathscr{O}]) \cong E[n]$*

Proof. The automorphisms of E as a torsor are the translation maps τ_P with $P \in E$. We see that $\tau_P^*(n\cdot\mathscr{O}) \sim n\cdot\mathscr{O}$ if and only if $P \in E[n]$. □

For some divisor class pair $(C,[A])$, the corresponding n-covering is (C,π) where

$$\begin{aligned} \pi : C &\longrightarrow \mathrm{Pic}^0(C) \cong E \\ P &\longmapsto [n\cdot P - A] \end{aligned}$$

To compute the Cassels-Tate pairing (7.1), we now want to be able to compute pushout forms on n-coverings of E. We do this by providing a solution to Problem 3.6.1. Let R be the étale algebra attached to $E[n]\setminus\{\mathscr{O}\}$. Let $(C,[A])$ be a torsor divisor class pair corresponding to some $\xi \in H^1(K,E[n])$. Recall that we have the following maps.

$$\mathrm{sum} : \mathrm{Pic}^0(C) \cong E \tag{7.2}$$

From [Sil08, Proposition X.3.2], there exists some P_0 on C such that

$$\begin{aligned} \theta : E &\longrightarrow C \\ P &\longmapsto P + P_0 \end{aligned} \tag{7.3}$$

is an isomorphism defined over $K(P_0)$. Thus sum is given by $[A_1 - A_2] \mapsto A_1 - P_0 - (A_2 - P_0) = A_1 - A_2$. From the short exact sequence

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{[n]} E \longrightarrow 0$$

we obtain

$$E(K) \xrightarrow{\delta} H^1(K,E[n]) \xrightarrow{\iota} H^1(K,E)$$

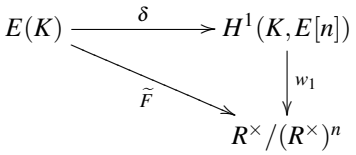
where

$$\begin{aligned} \delta(P) &= (E,[(n-1)\mathscr{O}+P]) \\ \iota(C,[A]) &= C. \end{aligned} \tag{7.4}$$

For n prime, we also have from Definition 3.4.1 the injection $w_1 : H^1(K,E[n]) \to R^\times/(R^\times)^n$, and in Proposition 3.4.8 we saw that in this case

$$\widetilde{F} = w_1 \circ \delta : E(K) \longrightarrow R^\times/(R^\times)^n$$

is given by $F \in R(E)^\times$ such that $\mathrm{div}(F_T) = n\cdot(T) - n\cdot(\mathscr{O})$ for all $T \in E[n]$. We extend to a map on divisors with support disjoint from $E[n]$ by letting $\widetilde{F} = F \circ \mathrm{sum}$. The following diagram then commutes.



Recall that we have $\mathscr{R} = \mathrm{Spec}(K[R])$ as in Section 3.4.2. Let $\xi \in H^1(K,E[n])$ with C_ξ its associated n-covering, and let $w_1(\xi) = \alpha \in R^\times/(R^\times)^n$. Then the K-rational points on C_ξ map to the points in $E(K)$ with image under δ given by ξ. The image under $\widetilde{F} = w_1 \circ \delta$ is therefore given by $\alpha(R^\times)^n$. We can therefore define the covering curve by

$$\{(P,z) \in E \times \mathscr{R} \mid F(P) = \alpha z^n\}.$$

We now work over $\overline{K}$ and write z_T for $z(T)$ as in Section 3.4.2. This signifies for $T \in E[n]$ the value of $z \in \overline{R}$ at T. We can use the z_T as coordinates on $\mathscr{R}$. This leads us to the following lemma on n-coverings of E.

Lemma 7.1.3. *Let $(C,[A])$ be the torsor divisor class pair corresponding to some $\xi \in H^1(K,E[n])$. Let C_ξ be the n-covering corresponding to ξ, and let $w_1(\xi) = \alpha$ mod $(R^\times)^n$. For $T \in E[n]$ let z_T be the coordinate function defined in Section 3.4.2 and given by evaluating at T. Then*

$$F_T(P) = \alpha(T) z_T^n$$

gives a degree n^2 embedding of C_ξ into $\mathbb{P}^{n^2-1}$.

Proof. This follows from the discussion in Section 2.5 of [CFO+12]. □

Recall also the embedding given by Proposition 3.4.11, which gives an embedding of C_ξ into $\mathbb{P}^{n^2-1}$ with section $n \cdot A$ (see Section 6 of [CFO+09]). Associated to that embedding is the element ρ corresponding to α in the following manner. There exists some $\gamma \in \overline{R}^\times$ such that $\alpha = \gamma^n$ and $\rho = \partial\gamma$. We now move on to the actual calculation of a pushout form, which we do in the spirit of Section 3.6.

7.1.2 Calculating a Pushout Form

Suppose we have $\xi, \xi' \in H^1(K,E[n])$ given by the torsor divisor class pairs $(C,[A])$ and $(C',[A'])$, respectively. Assume we have some $P \in E(K)$ such that

$$\begin{aligned}(C',[A']) &= (C,[A]) + \delta(P) \\ &= (C,[A]) + (E,[(n-1)\mathscr{O} + P]).\end{aligned}$$

Recall we have θ from (7.3) such that

$$(C',[A']) = (C,[A]) + (C,[(n-1)P_0 + (P+P_0)])$$

and if we apply ι from (7.4) we have $C' = C + C$. From [Sil08, Exercise 10.2] it follows that C' and C are in the same torsor class of $WC(E/K)$, therefore they are isomorphic over K and without loss of generality we assume $C' = C$. Thus $\mathrm{sum}([A' - A]) = P$.

If we now let $P = U \in E[n]$, we have $\mathrm{sum}(n \cdot [A' - A]) = \mathscr{O}$, therefore $n \cdot A$ and $n \cdot A'$ are linearly equivalent. We now want to show that if we can find an isomorphism $\psi : (C,[A]) \to (C,[A'])$ explicitly as a linear change of coordinates, then we can construct a pushout form. Assume we have such a ψ. Let $\iota_A : C \hookrightarrow$

$\mathbb{P}^{n^2-1}$ and $\iota_{A'} : C \hookrightarrow \mathbb{P}^{n^2-1}$ be the embeddings of C by $|n \cdot A|$ and $|n \cdot A'|$, respectively. The image of these embeddings is the same curve of degree n^2. Let g be a linear form associated to A', and we embed g^n into $\mathbb{P}^{n^2-1}$ using $\iota_{A'}$. We then apply ψ^{-1}, which because it is a linear change of coordinates takes $\iota_{A'}(g^n)$ to some $\iota_A(f(x_1,\ldots,x_n))$ with $\operatorname{div}\left(\frac{f}{g^n}\right) = n \cdot A - n \cdot A'$. We can in fact use any linear form for g, which will allow us to find a pushout form with a linearly equivalent divisor. If we have defined variables $x_1,\ldots,x_n$, we will therefore use $g = x_1$ in our calculations for simplicity's sake.

Lemma 7.1.4. *Let $\xi \in H^1(K, E[n])$ be represented by some torsor divisor class pair $(C,[A])$, as well as $w_1(\xi) = \alpha \in R^\times/(R^\times)^n$ and $w_2(\xi) = \rho \in (R \otimes R)^\times/\partial R^\times$ for $R = \operatorname{Maps}_K(E[n], \overline{K})$, as in Definition 3.4.1. Let $(C,[A'])$ be given as above by $(C,[A']) = (C,[A]) + \delta(P)$ for some $P \in E[n]$. Let the embedding of $(C,[A])$ into $\mathbb{P}^{n^2-1}$ be given by Lemma 7.1.3. Then the isomorphism $\psi : (C,[A]) \longrightarrow (C,[A'])$ can be given by a linear change of coordinates. Moreover, this change of coordinates can be given by*

$$\widetilde{z}_T = \frac{1}{\rho(T,-U)} \cdot \frac{z_{T-U}}{z_{-U}}.$$

Proof. From Lemma 7.1.3, we find the embeddings

$$F_T(P) = \alpha(T) z_T^n \qquad\qquad \widetilde{F}_T(P) = \widetilde{\alpha}(T) \widetilde{z}_T^n$$

for $(C,[A])$ and $(C,[A'])$, respectively. Recall from Lemma 3.4.6 that there exists some $\rho \in (R \otimes R)^\times/\partial R^\times$ such that

$$\partial\alpha(T_1,T_2) = \frac{\alpha(T_1)\alpha(T_2)}{\alpha(T_1+T_2)} = \rho(T_1,T_2)^n$$

for all $T_1, T_2 \in E[n]$. Because $(C,[A])$ and $(C,[A'])$ differ by $\delta(U)$ for $U \in E[n]$, we have

$$\widetilde{\alpha}(T) = F_T(U)\alpha(T)$$
$$\widetilde{F}_T(P) = F_T(P+U).$$

From the definition of F, we have

$$F_T(P+U) = F_T(U) \cdot \frac{F_{T-U}(P)}{F_{-U}(P)}$$

and so we obtain

$$\begin{aligned} F_T(P+U) &= F_T(U) \cdot \frac{\alpha(T-U) z_{T-U}^n}{\alpha(-U) z_{-U}^n} \\ &= \widetilde{\alpha}(T) \cdot \frac{\alpha(T-U)}{\alpha(T)\alpha(-U)} \left(\frac{z_{T-U}}{z_{-U}}\right)^n. \end{aligned}$$

Therefore we can take the following change of coordinates

$$\widetilde{z}_T = \frac{1}{\rho(T,-U)} \cdot \frac{z_{T-U}}{z_{-U}}. \tag{7.5}$$

□

This same change of coordinates can be used when we consider instead the embedding given by Proposition 3.4.11. Recall that in that case all the quadrics given in that proposition come from relation (3.25), which is

$$r_{(T_1,T_2)}(\pi(P)) z_{\mathcal{O}} z_{T_1+T_2} = \rho(T_1,T_2) z_{T_1} z_{T_2}.$$

Recall also that, as is described in Definition 3.4.1, we have some $\gamma \in \overline{R}^{\times}$ such that

$$\alpha = \gamma^n \qquad\qquad \rho = \partial\gamma.$$

We choose $\widetilde{\rho}$ such that $\widetilde{\rho} = r_{(T_1,T_2)}(U') \cdot \rho$ where $\pi(U') = U$ for some $U \in E[n]$ and thus we also have

$$\widetilde{r}_{(T_1,T_2)}(\pi(P))\widetilde{z}_{\mathscr{O}}\widetilde{z}_{T_1+T_2} = \widetilde{\rho}(T_1,T_2)\widetilde{z}_{T_1}\widetilde{z}_{T_2}.$$

We now want to show that the change of coordinates given by (7.5) is also the correct one to take in this situation. We know that

$$\widetilde{r}_{(T_1,T_2)}(\pi(P)) = r_{(T_1,T_2)}(\pi(P) + U').$$

Also, because $\operatorname{div}(r_{(T_1,T_2)}) = (T_1) + (T_2) - (T_1+T_2) - (\mathscr{O})$ we have

$$r_{(T_1,T_2)}(\pi(P)+U') = r_{(T_1,T_2)}(U') \cdot \frac{r_{T_1-U,T_2-U}(P)\, r_{T_1+T_2+U,U}(P)}{r_{U,-U}(P)}.$$

Therefore the following calculation shows that the change of coordinates (7.5) is indeed the correct one to take in the case of the embedding given by Proposition 3.4.11.

$$\begin{aligned}
\widetilde{r}_{(T_1,T_2)}(\pi(P)) &= r_{(T_1,T_2)}(U') \cdot \frac{\rho(T_1-U,T_2-U)\rho(T_1+T_2+U,U)}{\rho(U,-U)} \cdot \frac{z_{T_1-U} z_{T_2-U} z_{T_1+T_2+U} z_U}{z_{T_1+T_2+U} z_{T_1+T_2-U} z_U z_{-U}} \\
&= r_{(T_1,T_2)}(U') \cdot \frac{\rho(T_1,-U)\rho(T_2,-U)\rho(T_1-U,T_2-U)\rho(T_1+T_2+U,U)}{\rho(U,-U)\rho(T_1+T_2,-U)} \cdot \frac{\widetilde{z}_{T_1}\widetilde{z}_{T_2}}{\widetilde{z}_{T_1+T_2}} \\
&= r_{(T_1,T_2)}(U') \cdot \frac{\gamma(T_1)\gamma(T_2)}{\gamma(T_1+T_2)} \cdot \frac{\widetilde{z}_{T_1}\widetilde{z}_{T_2}}{\widetilde{z}_{T_1+T_2}} \\
&= r_{(T_1,T_2)}(U') \cdot \rho(T_1,T_2) \cdot \frac{\widetilde{z}_{T_1}\widetilde{z}_{T_2}}{\widetilde{z}_{T_1+T_2}} \\
&= \widetilde{\rho}(T_1,T_2) \cdot \frac{\widetilde{z}_{T_1}\widetilde{z}_{T_2}}{\widetilde{z}_{T_1+T_2}}.
\end{aligned}$$

This change of coordinate map was implemented in MAGMA by T. Fisher, and this is what is used in the next section. The following section calculates an example taken from Chapter 6.

7.2 Examples

We demonstrate this method using a small example first.

Example 7.2.1. We let $E : y^2 = x^3 + (-19x+8)^2$. Let $\phi : E \to \hat{E}$ be the 3-isogeny with kernel generated by $\langle (0,8) \rangle$. Let $L = \mathbb{Q}(\zeta_3)$ and $M = \mathbb{Q}(\zeta_3, \beta)$ where $\beta^3 = 31 \cdot 223$. Then the Selmer groups are given by

$$\begin{aligned}
S^{(\phi)}(E/\mathbb{Q}) &= \langle -186\zeta_3 - 155, -497736\zeta_3 + 131347 \rangle \subset L^{\times}/(L^{\times})^3 \\
S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) &= \langle 2 \rangle \subset \mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^3
\end{aligned}$$

We know without calculation that the Cassels-Tate pairing on $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) \times S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ must be trivial as this Selmer group consists of only one generator. The initial rank upper bound is therefore 2. Thus we obtain the generators $\langle g_1, g_2, g_3 \rangle$ for the Selmer group $S^{(3)}(E/\mathbb{Q})$ as follows. Using Lemma 2.5.10, we identify $H^1(\mathbb{Q}, E[3])$ with a certain subgroup H of pairs in $\mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^3 \times M^{\times}/(M^{\times})^3$. The element g_3 is

obtained by lifting 2 to $(2,b) \in H$, using Lemma 2.5.12. This lift may then be changed by any element in $(L^\times/(L^\times)^3)^-$ to obtain some curve that is everywhere locally soluble. The only primes we need to consider in choosing an element to alter the lift by are the bad primes of E, together with the ramified primes of L and any primes in the factorisation of the b.

$$g_1 = (1, G_1) = (1, -186\zeta_3 - 155)$$
$$g_2 = (1, G_2) = (1, -497736\zeta_3 + 131347)$$
$$g_3 = (2, \frac{1}{3}(249\zeta_3 + 115)\beta^2 + \frac{1}{3}(-2547\zeta_3 - 4730)\beta + \frac{1}{3}(-41478\zeta_3 + 48775)$$

which give the following covering curves

Selmer element	covering curve
g_1	$2x^3+5x^2y+10x^2z-xy^2+9xyz+8xz^2-2y^3+4y^2z+6yz^2-6z^3=0$
g_2	$-x^3-x^2y+x^2z+6xy^2+7xyz+6xz^2-2y^3-18y^2z-6yz^2+2z^3=0$
g_3	$-x^3-x^2y+x^2z+6xy^2+7xyz+6xz^2-2y^3-18y^2z-6yz^2+2z^3=0$

The pushout forms we obtain are given by

Selmer element	pushout form
g_1	$3x^2y+6x^2z-4xy^2-4xyz+2xz^2-4y^3+8yz^2-8z^3$
g_2	$x^2y-2x^2z+2xy^2-7xyz+4xz^2-2y^3-6y^2z+22yz^2+14z^3$
g_3	$x^3+3x^2y+2x^2z-2xy^2+4xyz+xz^2-12y^3-6y^2z+yz^2$

The primes over which we must take the local pairing are the bad primes of E together with the prime at 3. Thus we obtain the set $P = \{2,3,31,223\}$. This set is not enlarged by the pushout forms in this case. We found the following local points on each covering curve.

Selmer element	mod 2^4	mod 3^3	mod 31^3	mod 223^3
g_1	$(14:1:2)$	$(6:26:1)$	$(11731:16209:1)$	$(3860370:6805130:1)$
g_2	$(8:7:1)$	$(25:1:1)$	$(4674:27405:1)$	$(5766394:9588079:1)$
g_3	$(8:1:1)$	$(11:4:1)$	$(645:22070:1)$	$(8503491:7255590:1)$

Filling these in our pushout forms gives the following pairing elements.

Selmer element	mod 2^3	mod 3^4	mod 31^3	mod 223^3
g_1	4	54	8462	10987468
g_2	5	70	23207	1954722
g_3	5	49	15116	8013901

In this case we find only the primes 31 and 223 yield nonzero matrices. We choose the prime $p_{31} = 6+\zeta_3$ lying over 31 and $p_{223} = 11\zeta_3 - 6$ lying over 223 and use Remark 3.2.4. The following tables give the necessary information to calculate the local pairing.

$(a,b)_{p_{31}}$	$\mathrm{val}_{p_{31}}(a)$	$\mathrm{val}_{p_{31}}(b)$	c	$\left(\frac{c}{p_{31}}\right)$
$(G_1,8462)_{p_{31}}$	2	0	$\frac{1}{71605444}$	0
$(G_2,8462)_{p_{31}}$	1	0	$\frac{1}{8462}$	0
$(G_1,23207)_{p_{31}}$	2	0	$\frac{1}{538564849}$	1
$(G_2,23207)_{p_{31}}$	1	0	$\frac{1}{23207}$	2
$(G_1,15116)_{p_{31}}$	2	0	$\frac{1}{228493456}$	1
$(G_2,15116)_{p_{31}}$	1	0	$\frac{1}{15116}$	2

	g_1	g_2	g_3
G_1	0	2	2
G_2	0	1	1

$(a,b)_{p_{223}}$	$\mathrm{val}_{p_{223}}(a)$	$\mathrm{val}_{p_{223}}(b)$	c	$\left(\frac{c}{p_{223}}\right)$
$(G_1,10987468)_{p_{223}}$	0	0	1	0
$(G_2,10987468)_{p_{223}}$	2	0	$\frac{1}{120724453051024}$	2
$(G_1,1954722)_{p_{223}}$	0	0	1	0
$(G_2,1954722)_{p_{223}}$	2	0	$\frac{1}{3820938097284}$	1
$(G_1,8013901)_{p_{223}}$	0	0	1	0
$(G_2,8013901)_{p_{223}}$	2	0	$\frac{1}{64222609237801}$	1

	g_1	g_2	g_3
G_1	0	0	0
G_2	1	2	2

The Cassels-Tate pairing is now given by adding together the matrices thus obtained. The final pairing is given by the following matrix. Notice how the first two columns give a skew-symmetric pairing, as we would expect seeing as they come from lifting elements from $S^{(\phi)}(E/\mathbb{Q})$ rather than $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$. The matrix is of rank 2, therefore the elliptic curve E has rank 0.

	g_1	g_2	g_3
G_1	0	2	2
G_2	1	0	0

Example 7.2.2. Let $E = E_{12}(-3482, 1213)$. In this case, the Selmer groups are given by

$$\begin{aligned} S^{(\phi)}(E/\mathbb{Q}) =& \langle 335564343193791720\zeta_3 - 1532347698526352571, 566898402252\zeta_3 + 328319297033, \\ & 559524\zeta_3 + 33305\rangle = \langle g_1, g_2, g_3\rangle \subset L^\times/(L^\times)^3 \\ S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) =& \langle 2^2\cdot 29^2\cdot 1741\cdot 2269, 1213\cdot 1741^2\cdot 468817\rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^3 \end{aligned}$$

Because of the larger generators involved in computing the pairing on $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})\times S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$, we instead opted to use the method from this chapter to show that this curve cannot have rank greater than 2. We lifted the three generators of $S^{(\phi)}(E/\mathbb{Q})$ to $S^{(3)}(E/\mathbb{Q})$, and expressed them as covering curves as follows.

generator	covering curve
g_1	$\begin{aligned} &483284192300x^3 + 222070179765x^2y + 11438942216687x^2z - 1227782397135xy^2 \\ &+11438942216687xyz - 483284192300y^3 + 11438942216687y^2z + 11358133060446237z^3 = 0\end{aligned}$
g_2	$\begin{aligned} &159074538280x^3 + 580831373325x^2y + 11438942216687x^2z - 1058054988165xy^2 \\ &-11438942216687xyz + 159074538280y^3 + 11438942216687y^2z + 24669275234116737z^3 = 0\end{aligned}$
g_3	$\begin{aligned} &-2700898919390x^3 - 5577703949895x^2y + 11438942216687x^2z + 13680400708065xy^2 \\ &-11438942216687xyz - 2700898919390y^3 + 11438942216687y^2z + 146371783680291z^3 = 0\end{aligned}$

The pushout forms are then given by the following table.

generator	pushout form
g_1	$100790434931190274569327738926644 75x^3 - 131196564246607326335191542816370 20x^2y$ $+761687209124972454008225166358429809x^2z - 100053748807677802187688660360214695xy^2$ $-4972947514916959111016440758437520 66xyz + 367936002687996211396815296820445965xz^2$ $-937140377428464841628760996327431 00y^3 - 161730883871770447069499784650776514 1y^2z$ $-537265378161899097732921004146435552 90yz^2 + 134756653432870793383547645223575 1z^3$
g_2	$37404941266746860204131055392 45x^3 - 144879911470511455941993620884 50x^2y$ $-111819662826115600035764530367102x^2z + 313058904028278119909372153359 65xy^2$ $-781033288704484586154943316362723xyz + 122537142117848959148024732163597 15xz^2$ $-569380193119376820351629156788 0y^3 + 481593988949258975725538355432 73y^2z$ $-121123050084739806548135892145622 85yz^2 - 330943627077843380735477298266z^3$
g_3	$70657178574343890456052974402618316x^3 - 320623068884477139270258457737180363x^2y$ $-364045668872148013227435685272044531x^2z + 411592995267101686659815505534418608xy^2$ $+704007784990008293433421958890549832xyz + 160858900656105615798882342851476733 4xz^2$ $-148255831015343172568545792061662581y^3 - 189593629273458000816143782763407547y^2z$ $-130376945566080360350671947075612987 3yz^2 + 461664698271219161532934299283460 37z^3$

By following the same procedure as in the previous example, we find that the set of primes where the local pairing is nontrivial is given by $P = \{3, 7, 13, 67, 6661, 84589\}$. The following matrix gives the Cassels-Tate pairing.

	g_1	g_2	g_3
g_1	0	1	0
g_2	2	0	2
g_3	0	1	0

The rank of this matrix is 2, therefore the rank of E can be no larger than 2.

Example 7.2.3. We let $E = E_9(-1051, 1035)$ and $L = \mathbb{Q}(\zeta_3)$. We also have $M = \mathbb{Q}(\zeta_3, \beta)$ where $\beta^3 = 557 \cdot 18472823$. Then we have the Selmer groups

$$S^{(\phi)}(E/\mathbb{Q}) = \langle -80819560710\zeta_3 - 4966462801 \rangle = \langle G \rangle \subset L^\times/(L^\times)^3$$
$$S^{(\hat{\phi})}(\hat{E}/\mathbb{Q}) = \langle 2^2 \cdot 3^2 \cdot 5^2 \cdot 7, 2 \cdot 5 \cdot 149, \cdot 2 \cdot 7^2 \cdot 23, 5 \cdot 7 \cdot 1051 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^3$$

where the Selmer groups are calculated using Theorem 2.6.3. By our calculations in Chapter 6, all of these elements lift to elements of the Selmer group $S^{(3)}(E/\mathbb{Q})$. This group can be given as the subgroup H from Lemma 2.5.10. We lift some $a \in S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ to $(a,b) \in H$ using Lemma 2.5.12, and then changing this lift by an element $c \in (L^\times/(L^\times)^3)^-$. Let P be the set of primes given by the bad primes of E, the ramified primes of L and the primes present in b. Then c can be calculated from this set P. To save on compuation, we will consider only the following elements.

label	Original Element	Element of H
g_1	$-80819560710\zeta_3 - 4966462801$	$(1, -80819560710\zeta_3 - 4966462801)$
g_2	6300	$\big(6300, \frac{1}{3}(-97438867\zeta_3 - 69553013)\beta^2 + \frac{1}{3}(2007225593\zeta_3 - 10799492834)\beta + \frac{1}{3}(-100678111382 56\zeta_3 - 111897444673853)\big)$
g_3	2254	$\big(2254, \frac{1}{3}(-24850357506031\zeta_3 + 62216747799901)\beta^2 + \frac{1}{3}(25272141834079303\zeta_3 + 91826848470701060)\beta - 725363108512741682 54\zeta_3 + 8500537893454716079\big)$
g_4	1490	$\big(1490, (261239056\zeta_3 - 398747908)\beta^2 + (-1584172190224\zeta_3 - 1967141015996)\beta - 218209143895392\zeta_3 - 6082874424008356\big)$

We see that the element $2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 23 \cdot 149 \cdot 1051$ comes from one of the torsion points on $\hat{E}$, therefore will give a trivial pairing. Therefore we can omit $5 \cdot 7 \cdot 1051$, which will follow from the pairing on the remaining elements. This will save us computational time, as the changing of the lift by a suitable element of $(L^\times/(L^\times)^3)^-$ can be computationally heavy. The covering curves are given by

element	covering curves as element of $S^{(3)}(E/\mathbb{Q})$
g_1	$-9828x^3 - 2327x^2y - 1160649080x^2z + 27157xy^2 - 1160646753xyz + 1160658908xz^2 + 9828y^3 - 1160676237y^2z - 9828yz^2 + 1643329014701543 1480z^3 = 0$
g_2	$-157784415x^3 - 2318596466x^2y + 1880957611x^2z - 147345737xy^2 - 1082460515xyz + 2834244972xz^2 + 328366114y^3 + 2006774164y^2z - 1025326270yz^2 - 294530908z^3 = 0$
g_3	$-175149336x^3 - 434825264x^2y + 483372896x^2z - 1332721848xy^2 - 1546919209xyz + 5192895775xz^2 + 312609780y^3 + 939979002y^2z + 2150183535yz^2 - 850971807z^3 = 0$
g_4	$17921680x^3 - 108117634x^2y - 1243472112x^2z + 267939712xy^2 + 2136222223xyz - 8777934454xz^2 + 429061710y^3 + 469163827y^2z - 4492056088yz^2 + 29071705188z^3 = 0$

and the pushout forms are given by

element	pushout form
g_1	$1214243360x^3 + 760046426x^2y - 114403335021356x^2z - 1657941849xy^2 - 294290468647961xyz - 7436762090598914876xz^2 + 499043089y^3 + 183782392950311y^2z + 2447319594792481 4756yz^2 + 6714835765906705912z^3$
g_2	$6268065845586x^3 - 22803394894267x^2y - 132207383794789x^2z - 1239306365386928xy^2 + 408810156936579xyz + 694250487198389xz^2 + 1194060938823285y^3 - 785339260216356y^2z + 138926901666297yz^2 + 626807628254874z^3$
g_3	$507746424399560x^3 - 70612180843865x^2y + 2449728115111879x^2z + 1088810485223636xy^2 + 1424369443401917xyz + 345233497711969xz^2 - 114451650888048y^3 + 279867941288890y^2z + 188251854118882yz^2 - 121887521142680z^3$
g_4	$82142250644x^3 - 684345959332x^2y + 2494435616188x^2z + 2114173788528xy^2 + 364904200576xyz + 28292460960581xz^2 - 3949640775504y^3 - 15478632517146y^2z + 38028951847637yz^2 + 14777670989442z^3$

The bad primes of E are

$$P = \{2,3,5,7,13,19,23,73,149,181,557,1051,18472823\}$$

however the only primes contributing a nonzero part to the pairing are $\{19,73,181\}$. All three of these primes split, and we can choose the primes $p_{19} = -3\zeta_3 - 5$, $p_{73} = 8\zeta_3 - 1$ and $p_{181} = 11\zeta_3 - 4$ lying over them to calculate the local pairings, and then use Remark 3.2.4. The following table gives a local point on each covering curve for each prime.

Selmer element	mod 19^3	mod 73^3	mod 181^3
g_1	$(1113 : 4562 : 1)$	$(226224 : 249129 : 1)$	$(91 : 34 : 1)$
g_2	$(1096 : 2535 : 1)$	$(372251 : 388761 : 1)$	$(137 : 69 : 1)$
g_3	$(6153 : 6152 : 1)$	$(12644 : 42947 : 1)$	$(140 : 156 : 1)$
g_4	$(5054 : 2166 : 0)$	$(42632 : 367701 : 0)$	$(1428934 : 2783307 : 1)$

These we fill in on our pushout forms to obtain the following elements.

Selmer element	mod 19^3	mod 73^3	mod 181^4
g_1	5971	288103	5891
g_2	5118	139669	25553
g_3	1732	387855	20163
g_4	3366	202633	2061254

The following tables and matrices give the local pairing at each of our chosen primes.

$(a,b)_{p_{19}}$	$\mathrm{val}_{p_{19}}(a)$	$\mathrm{val}_{p_{19}}(b)$	c	$\left(\frac{c}{p_{19}}\right)$
$(G,5971)_{p_{19}}$	1	0	$\frac{1}{5971}$	1
$(G,5118)_{p_{19}}$	1	0	$\frac{1}{5118}$	0
$(G,1732)_{p_{19}}$	1	0	$\frac{1}{1732}$	1
$(G,3366)_{p_{19}}$	1	0	$\frac{1}{3366}$	1

	g_1	g_2	g_3	g_4
G_1	2	0	2	2

$(a,b)_{p_{73}}$	$\mathrm{val}_{p_{73}}(a)$	$\mathrm{val}_{p_{73}}(b)$	c	$\left(\frac{c}{p_{73}}\right)$
$(G,288103)_{p_{73}}$	2	0	$\frac{1}{83003338609}$	2
$(G,139669)_{p_{73}}$	2	0	$\frac{1}{19507429561}$	1
$(G,387855)_{p_{73}}$	2	0	$\frac{1}{150431501025}$	1
$(G,202633)_{p_{73}}$	2	0	$\frac{1}{41060132689}$	2

	g_1	g_2	g_3	g_4
G_1	1	2	2	1

$(a,b)_{p_{181}}$	$\mathrm{val}_{p_{181}}(a)$	$\mathrm{val}_{p_{181}}(b)$	c	$\left(\frac{c}{p_{181}}\right)$
$(G,5891)_{p_{181}}$	1	0	$\frac{1}{5891}$	0
$(G,25553)_{p_{181}}$	1	0	$\frac{1}{25553}$	2
$(G,20163)_{p_{181}}$	1	0	$\frac{1}{20163}$	1
$(G,2061254)_{p_{181}}$	1	0	$\frac{1}{2061254}$	0

	g_1	g_2	g_3	g_4
G_1	0	1	2	0

Computing the pairing using Definition 3.3.2 as before we add up the various local pairings, giving us the following matrix for the Cassels-Tate pairing.

	g_1	g_2	g_3	g_4
G_1	0	0	0	0

Thus we have not managed to improve the rank bound in this case.

Unfortunately, the computation proved too arduous to use in the case of $E_{12}(3097, 1872)$ and $E_{12}(-7189, 1452)$.

Chapter 8

Higher Descents and the Cassels-Tate Pairing

So far, we have been working only with curves admitting a 3-isogeny. In this chapter, we show how the pushout form method can be generalised and used in the case that we have a curve E with a rational 5-torsion point, of type $\mathbb{Z}/5\mathbb{Z}$-nonsplit.

Proposition 8.0.1. *Every elliptic curve $E/\mathbb{Q}$ with a rational point of order 5 can be written in the form*

$$y^2 + (1-\lambda)xy - \lambda y = x^3 - \lambda x^2$$

with $P = (0,0)$ a point of order 5.

Proof. As in Theorem 6.0.1, let $E : y^2 + (1-c)x - by = x^3 - bx^2$ with $P = (0,0)$ a point of order 5. Set $3P = -2P$ to obtain $b = c$ as required. □

Let G be the subgroup of $GL_2(\mathbb{Z}/5\mathbb{Z})$ through which the action of G_K on $E[5]$ factors. In this case, we have E such that $E[5]$ is generated by $\langle S, T\rangle$ with $G = \langle \sigma, \tau\rangle$ such that

$$\begin{aligned} \sigma(S) &= S & \tau(S) &= S \\ \sigma(T) &= S+T & \tau(T) &= 2T. \end{aligned}$$

Let $M = \mathbb{Q}(T)$, a number field of degree 20, and $L = \mathbb{Q}(\zeta_5)$, the degree 4 cyclotomic number field with ζ_5 a fifth root of unity. Let $M^{\langle\tau\rangle}$ be the subfield of M fixed by τ. We let ϕ be the isogeny with kernel generated by S. Then $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ is a subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^5$ and to compute the Cassels-Tate pairing on it, we must lift each element in $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ to some element of $H^1(\mathbb{Q}, E[5])$. This we can do using Lemma 2.5.12. For each element $a \in S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$, we solve the norm equation $N_{M/L}(\xi) = a$. The lemma then gives us the lift as the pair $(a,b) \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^5 \times M^\times/(M^\times)^5$ where b is given by

$$b = \frac{\sigma(\eta)\sigma^2(\eta)^2}{\sigma^4(\eta)\sigma^3(\eta)^2} \tag{8.1}$$

where $\eta = N_{M/M^{\langle\tau\rangle}}(\xi)$. Following [Vél71], we have the following curve $\hat{E}$ such that the isogeny $\phi : E \to \hat{E}$ has kernel $\langle S\rangle$.

$$\hat{E} : y^2 + (1-\lambda)xy - \lambda y = x^3 - \lambda x^2 - 5\lambda(\lambda^2 + 2\lambda - 1)x - \lambda(\lambda^4 + 10\lambda^3 - 5\lambda^2 + 15\lambda - 1)$$

Unfortunately, we were not able to improve the method of solving norm equations in this case as we were in the $p = 3$ case. This will therefore be the major bottleneck in all our computations and severely limit the number of examples we can do.

The covering curve represented by u is given by a curve in $\mathbb{P}^4$ defined by 5 quadrics as in [Fis03].

$$C_u = \left\{ \begin{array}{l} \frac{\lambda}{u}x_0^2 + x_3x_4 - x_1x_2 = 0 \\ x_1^2 + x_0x_3 - ux_2x_4 = 0 \\ ux_2^2 - x_0x_4 - x_1x_3 = 0 \\ x_3^2 - x_1x_4 + \lambda x_0x_2 = 0 \\ x_4^2 - x_2x_3 - \frac{\lambda}{u}x_0x_1 = 0 \end{array} \right\} \tag{8.2}$$

The formula for the pushout form is constructed as in the $p = 3$ case from Section 3.5. We use Proposition 3.4.11 to set up an ideal of 275 quadrics. We then define a suitable linear form and take its fifth power, and eliminate all but 5 variables. The following subsections deal with how this is done.

8.1 Computing ρ in the $\mathbb{Z}/5\mathbb{Z}$-nonsplit Case

Let $R = \mathbb{Q} \times M$ where $M = \mathbb{Q}(T) = \mathbb{Q}(\zeta_5, \beta)$ where β is the root of some degree 5 polynomial. Then we saw in Section 3.4 that we can express $u \in S^{(5)}(E/\mathbb{Q})$ as either $\alpha \in R^\times/(R^\times)^5$ or as $\rho \in (R \otimes R)^\times/\partial R^\times$. In this section, given some element of $H^1(\mathbb{Q}, E[5])$ in the form α, we calculate ρ explicitly.

From Lemma 3.4.6, we have that $\rho^5 = \partial\alpha$. To obtain ρ, we find all fifth roots of $\partial\alpha$ in $\mathrm{Sym}^2(R)$. We then use the remaining conditions of Lemma 3.4.6 to eliminate candidates until only one remains. In this case, ρ will be unique. This follows from the fact that we saw in Section 3.4 that there exists some $\gamma \in \overline{R}^\times$ such that $\alpha = \gamma^5 \in R^\times$ and $\rho = \partial\gamma \in (R \otimes R)^\times$. The number of choices for ρ is given by $\#(\partial\Gamma) = \frac{\#\Gamma}{5^2} = 1$. This may not be the case in different situations.

There are 55 orbits for the action of G on $E[5] \times E[5]$, with representatives given in the following table. Let $\alpha = (a, b) \in R^\times$ be the representative of some element of $H^1(E[5], \mathbb{Q})$. Usually, we have a the representative of some element in $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ and b is given by (8.1). Thus we have $\alpha(S) = a$ and $\alpha(T) = b$ in what follows here. We use that ρ is symmetric and that $\rho(\mathscr{O}, T_i) = 1$ for all $T_i \in E[5]$. The variables k_i, l_i, m_i, n_i, p_i are unknowns to be determined. They satisfy the following.

$$k_i^5 = \frac{a^i b}{\sigma^i(b)} \qquad l_i^5 = \frac{b\sigma^{i-1}(b)}{\tau\sigma^{i-1}(b)} \qquad m_i^5 = \frac{b\tau\sigma^{i-1}(b)}{\tau^3\sigma^{i-1}(b)}$$

$$n_i^5 = \frac{b\tau^3\sigma^{i-1}(b)}{\tau^2\sigma^{i-1}(b)} \qquad p_i^5 = \frac{b\sigma^{i-1}\tau^2(b)}{a^{i-1}}$$

#	(T_1,T_2)	T_1+T_2	ρ	#	(T_1,T_2)	T_1+T_2	ρ
1	$(\mathscr{O},\mathscr{O})$	$\mathscr{O}$	1	29	$(3S,T)$	$3S+T$	k_3
2	$(\mathscr{O},S)$	S	1	30	$(4S,T)$	$4S+T$	k_4
3	$(\mathscr{O},2S)$	$2S$	1	31	$(T,\mathscr{O})$	T	1
4	$(\mathscr{O},3S)$	$3S$	1	32	(T,S)	$S+T$	k_1
5	$(\mathscr{O},4S)$	$4S$	1	33	$(T,2S)$	$2S+T$	k_2
6	$(S,\mathscr{O})$	S	1	34	$(T,3S)$	$3S+T$	k_3
7	(S,S)	$2S$	1	35	$(T,4S)$	$4S+T$	k_4
8	$(S,2S)$	$3S$	1	36	(T,T)	$2T$	l_1
9	$(S,3S)$	$4S$	1	37	$(T,S+T)$	$S+2T$	l_2
10	$(S,4S)$	$\mathscr{O}$	a	38	$(T,2S+T)$	$2S+2T$	l_3
11	$(2S,\mathscr{O})$	$2S$	1	39	$(T,3S+T)$	$3S+2T$	l_4
12	$(2S,S)$	$3S$	1	40	$(T,4S+T)$	$4S+2T$	l_5
13	$(2S,2S)$	$4S$	1	41	$(T,2T)$	$3T$	m_1
14	$(2S,3S)$	$\mathscr{O}$	a	42	$(T,S+2T)$	$S+3T$	m_2
15	$(2S,4S)$	S	a	43	$(T,2S+2T)$	$2S+3T$	m_3
16	$(3S,\mathscr{O})$	$3S$	1	44	$(T,3S+2T)$	$3S+3T$	m_4
17	$(3S,S)$	$4S$	1	45	$(T,4S+2T)$	$4S+3T$	m_5
18	$(3S,2S)$	0	a	46	$(T,3T)$	$4T$	n_1
19	$(3S,3S)$	S	a	47	$(T,S+3T)$	$S+4T$	n_2
20	$(3S,4S)$	$2S$	a	48	$(T,2S+3T)$	$2S+4T$	n_3
21	$(4S,\mathscr{O})$	$4S$	1	49	$(T,3S+3T)$	$3S+4T$	n_4
22	$(4S,S)$	$\mathscr{O}$	a	50	$(T,4S+3T)$	$4S+4T$	n_5
23	$(4S,2S)$	S	a	51	$(T,4T)$	$\mathscr{O}$	p_1
24	$(4S,3S)$	$2S$	a	52	$(T,S+4T)$	S	p_2
25	$(4S,4S)$	$3S$	a	53	$(T,2S+4T)$	$2S$	p_3
26	$(\mathscr{O},T)$	T	1	54	$(T,3S+4T)$	$3S$	p_4
27	(S,T)	$S+T$	k_1	55	$(T,4S+4T)$	$4S$	p_5
28	$(2S,T)$	$2S+T$	k_2				

We have a number of choices for ρ, diminished by the following equations, which we obtained using part 3 of Lemma 3.4.6.

$$\begin{aligned}
\rho(T,2S)\rho(S,S)=\rho(T,S)\rho(S+T,S) &\quad\text{thus}\quad k_2=k_1\sigma(k_1)\\
\rho(T,3S)\rho(S,2S)=\rho(T,S)\rho(S+T,2S) &\quad\text{thus}\quad k_3=k_1\sigma(k_1)\sigma^2(k_1)\\
\rho(T,4S)\rho(S,3S)=\rho(T,S)\rho(S+T,3S) &\quad\text{thus}\quad k_3=k_4\sigma(k_1)\sigma^2(k_1)\sigma^3(k_1)\\
\rho(4S,2T)\rho(T,T)=\rho(4S,T)\rho(4S+T,T) &\quad\text{thus}\quad l_2=\tfrac{\sigma\tau(k_4)\sigma(l_1)}{\sigma(k_4)}\\
\rho(3S,2T)\rho(T,T)=\rho(3S,T)\rho(3S+T,T) &\quad\text{thus}\quad l_3=\tfrac{\sigma^2\tau(k_3)\sigma^2(l_1)}{\sigma^2(k_3)}\\
\rho(2S,2T)\rho(T,T)=\rho(2S,T)\rho(2S+T,T) &\quad\text{thus}\quad l_4=\tfrac{\sigma^3\tau(k_2)\sigma^3(l_1)}{\sigma^3(k_2)}\\
\rho(S,2T)\rho(T,T)=\rho(S,T)\rho(S+T,T) &\quad\text{thus}\quad l_5=\tfrac{\sigma^4\tau(k_1)\sigma^4(l_1)}{\sigma^4(k_1)}\\
\rho(2T,S+4T)\rho(4T,S)=\rho(2T,4T)\rho(T,S) &\quad\text{thus}\quad m_2=\tfrac{m_1\tau^3(k_1)}{\tau(k_1)}\\
\rho(2T,2S+4T)\rho(4T,2S)=\rho(2T,4T)\rho(T,2S) &\quad\text{thus}\quad m_3=\tfrac{m_1\tau^3(k_2)}{\tau(k_2)}\\
\rho(2T,3S+4T)\rho(4T,3S)=\rho(2T,4T)\rho(T,3S) &\quad\text{thus}\quad m_4=\tfrac{m_1\tau^3(k_3)}{\tau(k_3)}\\
\rho(2T,4S+4T)\rho(4T,4S)=\rho(2T,4T)\rho(T,4S) &\quad\text{thus}\quad m_5=\tfrac{m_1\tau^3(k_4)}{\tau(k_4)}\\
\rho(T,3T)\rho(T,2T)=\rho(T,T)\rho(2T,2T) &\quad\text{thus}\quad n_1=\tfrac{l_1\tau(l_1)}{m_1}\\
\rho(T,S+3T)\rho(T,S+2T)=\rho(T,T)\rho(2T,S+2T) &\quad\text{thus}\quad n_2=\tfrac{l_1\tau(l_2)}{m_2}
\end{aligned}$$

$$\begin{aligned}
\rho(T,2S+3T)\rho(T,2S+2T) &= \rho(T,T)\rho(2T,2S+2T) \quad \text{thus} \quad n_3 = \tfrac{l_1\tau(l_3)}{m_3}\\
\rho(T,3S+3T)\rho(T,3S+2T) &= \rho(T,T)\rho(2T,3S+2T) \quad \text{thus} \quad n_4 = \tfrac{l_1\tau(l_4)}{m_4}\\
\rho(T,4S+3T)\rho(T,4S+2T) &= \rho(T,T)\rho(2T,4S+2T) \quad \text{thus} \quad n_5 = \tfrac{l_1\tau(l_5)}{m_5}\\
b &= l_1m_1n_1p_1 \quad \text{thus} \quad p_1 = \tfrac{b}{l_1^2\tau(l_1)}\\
\rho(4T,S)\rho(T,S+4T) &= \rho(4T,T)\rho(O,S+4T) \quad \text{thus} \quad p_2 = \tfrac{\tau^2(p_1)}{\tau^2(k_1)}\\
\rho(4T,2S)\rho(T,2S+4T) &= \rho(4T,T)\rho(O,2S+4T) \quad \text{thus} \quad p_3 = \tfrac{\tau^2(p_1)}{\tau^2(k_2)}\\
\rho(4T,3S)\rho(T,3S+4T) &= \rho(4T,T)\rho(O,3S+4T) \quad \text{thus} \quad p_4 = \tfrac{\tau^2(p_1)}{\tau^2(k_3)}\\
\rho(4T,4S)\rho(T,4S+4T) &= \rho(4T,T)\rho(O,4S+4T) \quad \text{thus} \quad p_5 = \tfrac{\tau^2(p_1)}{\tau^2(k_4)}
\end{aligned}$$

We seem now to have three free choices of fifth roots, namely, k_1, l_1 and m_1. These satisfy the following

$$k_1^5 = \frac{ab}{\sigma(b)} \qquad l_1^5 = \frac{b^2}{\tau(b)} \qquad m_1^5 = \frac{b\tau(b)}{\tau^3(b)}.$$

But we have more conditions. First of all, we see that because $\rho(T,4T) = \rho(4T,T)$ we must have $\tau^2(p_1) = p_1$, which fixes the choice of root for p_1. We also have $\rho(T,2T) = \rho(2T,T)$ which gives us that $m_1 = \tau(n_1)$, fixing the choice of root for m_1. The last choice depends on the fact that $\rho(S,2T)\rho(T,T) = \rho(S,T)\rho(S+T,T)$, giving us that $\tau(k_1)l_1 = k_1\sigma(l_5)$, fixing the choice for k_1 as well. Thus we have determined ρ uniquely in this case.

8.2 The Pushout Form in the $\mathbb{Z}/5\mathbb{Z}$ Case

The pushout form in this case has very large coefficients. We were not able to simplify it as we did in the $p = 3$ case in Section 3.5. This is also the reason for the calculation in the previous section, as all our coefficients rely on ρ. We will not give the formula in full here, anyone interested in it may contact the author to obtain it electronically, or follow the computation given here.

Let our torsion points be labelled as follows.

$$\begin{array}{llll}
T_0 = \mathcal{O} & & & \\
T_1 = S & T_2 = 4S & T_3 = 2S & T_4 = 3S\\
T_5 = T & T_6 = 4T & T_7 = 2T & T_8 = 3T\\
T_9 = S+T & T_{10} = 4S+4T & T_{11} = S+2T & T_{12} = 4S+3T\\
T_{13} = S+4T & T_{14} = 4S+T & T_{15} = S+3T & T_{16} = 4S+2T\\
T_{17} = 2S+T & T_{18} = 3S+4T & T_{19} = 2S+2T & T_{20} = 3S+3T\\
T_{21} = 2S+4T & T_{22} = 3S+T & T_{23} = 2S+3T & T_{24} = 3S+2T
\end{array}$$

Let u be some element in $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$. Let $L = \mathbb{Q}(\zeta_5)$, a fifth root of unity, and $M = \mathbb{Q}(T) = \mathbb{Q}(\zeta_5,\beta)$ where β is the root of some degree 5 polynomial. We have that $\lambda_{i,j}$ is the slope between points T_i and T_j, x_i is the x-coordinate of the point T_i and $\rho_{i,j}$ is the element $\rho(T_i,T_j)$ as calculated in Section 8.1. Denote by z_i the coordinate function z_{T_i}.

We now compute the pushout form as described at the end of Section 3.4. Let

$$g = z_5 + z_9 + z_{17} + z_{22} + z_{14}.$$

We then compute g^5 and eliminate any terms involving coordinate functions other than z_0, z_1, z_2, z_3, z_4. This is done using Proposition 3.4.11. We simply replace every monomial occurring in g^5 with a suitable

alternative constructed from the quadrics generating the ideal I_D.

The resulting pushout form on C_u is given by a form in the following 31 monomials.

$$z_0^5, z_0^4z_1, z_0^4z_2, z_0^4z_3, z_0^4z_4, z_0^3z_1^2, z_0^3z_1z_2, z_0^3z_1z_3, z_0^3z_1z_4, z_0^3z_2^2, z_0^3z_3^2, z_0^3z_4^2, z_0^2z_1^3, z_0^2z_1^2z_2, z_0^2z_1^2z_3, z_0^2z_1^2z_4,$$
$$z_0^2z_1z_2^2, z_0^2z_1z_3^2, z_0^2z_1z_4^2, z_0z_1^4, z_0z_1^3z_2, z_0z_1^3z_3, z_0z_1^3z_4, z_0z_1^2z_2^2, z_0z_1^2z_3^2, z_0z_1^2z_4^2, z_1^5, z_1^4z_2, z_1^3z_2^2, z_1^3z_3^2, z_1^3z_4^2 \quad (8.3)$$

We give just five of the coefficients here, as amongst the remaining 21 are several coefficients that are several pages long. We therefore omit these and urge that interested parties contact the author.

The coefficient of the $z_1^3z_4^2$ term is $\mathrm{Tr}_{M/L}(\eta)$ where η is given by

$$60\frac{\rho_{4,4}\rho_{1,7}\rho_{1,15}\rho_{1,16}}{\rho_{5,5}\rho_{7,15}\rho_{14,17}\rho_{16,22}}+20\frac{\rho_{4,4}\rho_{1,7}\rho_{1,16}\rho_{1,23}}{\rho_{5,5}\rho_{5,9}\rho_{7,22}\rho_{16,23}}+10\frac{\rho_{4,4}\rho_{1,16}\rho_{1,20}\rho_{1,24}}{\rho_{5,5}\rho_{17,17}\rho_{5,16}\rho_{20,24}}+30\frac{\rho_{4,4}\rho_{1,8}\rho_{1,11}\rho_{1,16}}{\rho_{5,5}\rho_{9,9}\rho_{8,11}\rho_{16,17}}+5\frac{\rho_{4,4}\rho_{1,16}^2\rho_{1,21}}{\rho_{5,5}^2\rho_{16,16}\rho_{14,21}}$$

The coefficient of the $z_1^3z_3^2$ term is $\mathrm{Tr}_{M/L}(\eta)$ where η is given by

$$60\frac{\rho_{3,3}\rho_{1,16}\rho_{1,19}\rho_{1,23}}{\rho_{5,5}\rho_{9,17}\rho_{14,16}\rho_{19,23}}+20\frac{\rho_{3,3}\rho_{1,16}\rho_{1,19}\rho_{1,23}}{\rho_{5,5}\rho_{5,22}\rho_{14,16}\rho_{19,23}}+30\frac{\rho_{3,3}\rho_{1,15}\rho_{1,16}\rho_{1,24}}{\rho_{5,5}\rho_{17,17}\rho_{15,24}\rho_{16,22}}+10\frac{\rho_{3,3}\rho_{1,11}\rho_{1,16}\rho_{1,20}}{\rho_{5,5}\rho_{9,9}\rho_{5,16}\rho_{11,20}}+5\frac{\rho_{3,3}\rho_{1,16}^2\rho_{1,21}}{\rho_{5,5}^2\rho_{16,16}\rho_{17,21}}$$

The coefficient of the $z_1^3z_2^2$ term is $\mathrm{Tr}_{M/L}(\eta)$ where η is given by

$$20\frac{\rho_{2,2}\rho_{1,8}\rho_{1,16}\rho_{1,24}}{\rho_{5,5}\rho_{5,14}\rho_{8,24}\rho_{16,17}}+10\frac{\rho_{2,2}\rho_{1,7}\rho_{1,16}\rho_{1,20}}{\rho_{5,5}\rho_{22,22}\rho_{5,16}\rho_{7,20}}+60\frac{\rho_{2,2}\rho_{1,16}^2\rho_{1,21}}{\rho_{5,5}\rho_{16,16}\rho_{9,21}\rho_{17,22}}+30\frac{\rho_{2,2}\rho_{1,11}\rho_{1,16}\rho_{1,23}}{\rho_{5,5}\rho_{9,9}\rho_{11,23}\rho_{1416}}+5\frac{\rho_{2,2}\rho_{1,16}^2\rho_{1,21}}{\rho_{5,5}^2\rho_{16,16}\rho_{9,21}}$$

The coefficient of the $z_0z_1^2z_4^2$ term is $\mathrm{Tr}_{M/L}(\eta)$ where η is given by

$$\begin{aligned}
&-20\frac{\lambda_{5,5}\rho_{4,4}\rho_{1,8}\rho_{1,11}}{\rho_{5,5}\rho_{5,17}\rho_{7,9}\rho_{8,11}}-60\frac{\lambda_{5,5}\rho_{4,4}\rho_{1,15}\rho_{1,16}}{\rho_{5,5}\rho_{7,15}\rho_{9,14}\rho_{16,22}}-30\frac{\lambda_{5,5}\rho_{4,4}\rho_{1,20}\rho_{1,24}}{\rho_{5,5}\rho_{17,17}\rho_{7,14}\rho_{20,24}}-10\frac{\lambda_{5,5}\rho_{4,4}\rho_{1,12}\rho_{1,19}}{\rho_{5,5}\rho_{14,14}\rho_{5,7}\rho_{12,19}}\\
&-10\frac{\lambda_{5,5}\rho_{4,4}\rho_{1,16}\rho_{1,23}}{\rho_{5,5}^2\rho_{7,22}\rho_{16,23}}-10\frac{\lambda_{14,14}\rho_{4,4}\rho_{1,16}\rho_{1,20}}{\rho_{5,5}\rho_{14,14}\rho_{5,16}\rho_{20,24}}-5\frac{\lambda_{16,16}\rho_{4,4}\rho_{1,16}^2}{\rho_{5,5}^2\rho_{16,16}\rho_{18,22}}-30\frac{\lambda_{17,17}\rho_{4,4}\rho_{1,16}\rho_{1,23}}{\rho_{5,5}\rho_{17,17}\rho_{14,16}\rho_{16,23}}\\
&+20\frac{\lambda_{1,11}\rho_{4,4}\rho_{1,12}\rho_{1,16}}{\rho_{5,5}\rho_{5,17}\rho_{9,16}\rho_{12,19}}+20\frac{\lambda_{1,12}\rho_{4,4}\rho_{1,11}\rho_{1,16}}{\rho_{5,5}\rho_{5,17}\rho_{8,11}\rho_{9,16}}+60\frac{\lambda_{1,15}\rho_{4,4}\rho_{1,16}^2}{\rho_{5,5}\rho_{9,14}\rho_{16,22}\rho_{16,23}}+20\frac{\lambda_{1,16}\rho_{4,4}\rho_{1,8}\rho_{1,11}}{\rho_{5,5}\rho_{5,17}\rho_{7,9}\rho_{8,11}}\\
&+120\frac{\lambda_{1,16}\rho_{4,4}\rho_{1,15}\rho_{1,16}}{\rho_{5,5}\rho_{7,15}\rho_{9,14}\rho_{16,22}}+30\frac{\lambda_{1,16}\rho_{4,4}\rho_{1,20}\rho_{1,24}}{\rho_{5,5}\rho_{17,17}\rho_{7,14}\rho_{20,24}}+10\frac{\lambda_{1,16}\rho_{4,4}\rho_{1,12}\rho_{1,19}}{\rho_{5,5}\rho_{14,14}\rho_{5,7}\rho_{12,19}}+10\frac{\lambda_{1,16}\rho_{4,4}\rho_{1,16}\rho_{1,23}}{\rho_{5,5}^2\rho_{7,22}\rho_{16,23}}\\
&+10\frac{\lambda_{1,19}\rho_{4,4}\rho_{1,16}\rho_{1,20}}{\rho_{5,5}\rho_{14,14}\rho_{5,16}\rho_{20,24}}+10\frac{\lambda_{1,20}\rho_{4,4}\rho_{1,16}\rho_{1,19}}{\rho_{5,5}\rho_{14,14}\rho_{5,16}\rho_{12,19}}+5\frac{\lambda_{1,21}\rho_{4,4}\rho_{1,16}^2}{\rho_{5,5}^2\rho_{16,16}\rho_{18,22}}+30\frac{\lambda_{1,23}\rho_{4,4}\rho_{1,16}\rho_{1,24}}{\rho_{5,5}\rho_{17,17}\rho_{14,16}\rho_{20,24}}\\
&+30\frac{\lambda_{1,24}\rho_{4,4}\rho_{1,16}\rho_{1,23}}{\rho_{5,5}\rho_{17,17}\rho_{14,16}\rho_{16,23}}-10\frac{\lambda_{5,16}\rho_{4,4}\rho_{1,16}\rho_{1,19}}{\rho_{5,5}\rho_{14,14}\rho_{5,16}\rho_{12,19}}-20\frac{\lambda_{5,17}\rho_{4,4}\rho_{1,12}\rho_{1,16}}{\rho_{5,5}\rho_{5,17}\rho_{9,16}\rho_{12,19}}-60\frac{\lambda_{9,14}\rho_{4,4}\rho_{1,15}\rho_{1,16}}{\rho_{5,5}\rho_{7,15}\rho_{9,14}\rho_{16,22}}\\
&-20\frac{\lambda_{9,16}\rho_{4,4}\rho_{1,11}\rho_{1,16}}{\rho_{5,5}\rho_{5,17}\rho_{8,11}\rho_{9,16}}-30\frac{\lambda_{14,16}\rho_{4,4}\rho_{1,16}\rho_{1,24}}{\rho_{5,5}\rho_{17,17}\rho_{14,16}\rho_{20,24}}-60\frac{\lambda_{16,22}\rho_{4,4}\rho_{1,16}^2}{\rho_{5,5}\rho_{9,14}\rho_{16,22}\rho_{16,23}}
\end{aligned}$$

The coefficient of the $z_0z_1^3z_4$ term is $\mathrm{Tr}_{M/L}(\eta)$ where η is given by

$$20\frac{\lambda_{2,2}\rho_{1,8}\rho_{1,16}\rho_{1,24}}{\rho_{5,5}\rho_{5,14}\rho_{8,24}\rho_{16,17}}+10\frac{\lambda_{2,2}\rho_{1,7}\rho_{1,16}\rho_{1,20}}{\rho_{5,5}\rho_{22,22}\rho_{5,16}\rho_{7,20}}+60\frac{\lambda_{2,2}\rho_{1,16}^2\rho_{1,21}}{\rho_{5,5}\rho_{16,16}\rho_{9,21}\rho_{17,22}}+30\frac{\lambda_{2,2}\rho_{1,11}\rho_{1,16}\rho_{1,23}}{\rho_{5,5}\rho_{9,9}\rho_{11,23}\rho_{14,16}}$$
$$+5\frac{\lambda_{2,2}\rho_{1,16}^2\rho_{1,21}}{\rho_{5,5}^2\rho_{16,16}\rho_{9,21}}-10\frac{\lambda_{7,20}\rho_{1,7}\rho_{1,16}\rho_{1,20}}{\rho_{5,5}\rho_{22,22}\rho_{5,16}\rho_{7,20}}-20\frac{\lambda_{8,24}\rho_{1,8}\rho_{1,16}\rho_{1,24}}{\rho_{5,5}\rho_{5,14}\rho_{8,24}\rho_{16,17}}-60\frac{\lambda_{9,21}\rho_{1,16}^2\rho_{1,21}}{\rho_{5,5}\rho_{16,16}\rho_{9,21}\rho_{17,22}}$$
$$-5\frac{\lambda_{9,21}\rho_{1,16}^2\rho_{1,21}}{\rho_{5,5}^2\rho_{16,16}\rho_{9,21}}-30\frac{\lambda_{11,23}\rho_{16,16}\rho_{1,11}\rho_{1,16}\rho_{1,23}}{\rho_{5,5}\rho_{9,9}\rho_{16,16}\rho_{11,23}\rho_{14,16}}$$

8.3 Examples

Example 8.3.1. Let $\lambda=\frac{48}{5}$. Let $L=\mathbb{Q}(\zeta_5)$, the degree 4 cyclotomic field. Let $M=\mathbb{Q}(\zeta_5,\beta)$ where $\beta^5=\frac{1}{361}(650725\zeta_5^3+650725\zeta_5^2-402450)$. Then $E[5]$ is generated by $\langle S,T\rangle$ with

$$\begin{aligned}
S=&(0,0)\\
T=&\Bigg(\frac{1}{15625}(-10556\zeta_5^3-10556\zeta_5^2-16923)\beta^4+\frac{1}{3125}(-2329\zeta_5^3-2329\zeta_5^2-3623)\beta^3\\
&+\frac{1}{3125}(-5639\zeta_5^3-5639\zeta_5^2-8642)\beta^2+\frac{361}{625}\beta+\frac{1}{625}(-361\zeta_5^3-361\zeta_5^2-3003),\\
&\frac{1}{78125}(-567226\zeta_5^3-145949\zeta_5^2-259267\zeta_5-493478)\beta^4\\
&+\frac{1}{78125}(-24873\zeta_5^3-294211\zeta_5^2+181651\zeta_5-298647)\beta^3\\
&+\frac{1}{15625}(-202877\zeta_5^3-91872\zeta_5^2-52272\zeta_5-211939)\beta^2\\
&+\frac{1}{15625}(20938\zeta_5^3+32851\zeta_5^2+53789\zeta_5+65702)\beta\\
&+\frac{1}{3125}(-1805\zeta_5^3+19133\zeta_5^2+32851\zeta_5-33139)\Bigg).
\end{aligned}$$

We have σ such that $\sigma(T)=S+T$ and τ such that $\tau(T)=2T$. Thus $\tau(\zeta_5)=\zeta_5^2$ and $\sigma(\beta)=\zeta_5^3\beta$.

Using the method from Section 2.6 and Cassels' formula (6.1), we find that the Selmer groups we are interested in are given by

$$\begin{aligned}
S^{(\phi)}(E/\mathbb{Q})&=\langle 1\rangle\subset L^\times/(L^\times)^5\\
S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})&=\langle 2,3,5\rangle\subset\mathbb{Q}^\times/(\mathbb{Q}^\times)^5.
\end{aligned}$$

Thus an initial upper bound for the rank is 2. To use the formula partially given in Section 8.2, for every generator $g\in S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ we need to find ξ such that $N_{M/L}(\xi)=g$. The following table gives the solutions to these norm equations, found using MAGMA's NormEquation.

g	ξ
2	$\frac{1}{2375}(-1316\zeta_5^3-1316\zeta_5^2-2127)\beta^4+\frac{1}{2375}(704\zeta_5^3+704\zeta_5^2+1117)\beta^3$ $+\frac{1}{25}(17\zeta_5^3+17\zeta_5^2+27)\beta^2+\frac{1}{25}(-11\zeta_5^3-11\zeta_5^2-13)\beta-\frac{1}{5}$
3	$\frac{1}{2375}(2739\zeta_5^3+2739\zeta_5^2+4453)\beta^4+\frac{1}{2375}(-2816\zeta_5^3-2816\zeta_5^2-4468)\beta^3$ $+\frac{1}{25}(-68\zeta_5^3-68\zeta_5^2-108)\beta^2+\frac{1}{25}(-76\zeta_5^3-76\zeta_5^2-133)\beta-\frac{26}{5}$
5	$\frac{1}{2375}(-3948\zeta_5^3-3948\zeta_5^2-6381)\beta^4+\frac{1}{2375}(2112\zeta_5^3+2112\zeta_5^2+3351)\beta^3$ $+\frac{1}{25}(51\zeta_5^3+51\zeta_5^2+81)\beta^2+\frac{1}{25}(-33\zeta_5^3-33\zeta_5^2-39)\beta-\frac{8}{5}$

We can use the table above to construct the pushout forms. We calculate ρ as described in Section 8.1 and then simply fill in the coefficients, some of which are provided in Section 8.2. The pushout forms are linear combinations of the monomials in (8.3) with coefficients in L. Unfortunately in this case they are too large to reproduce here. We then proceed as in Section 5.2. The pairing is calculated by finding the sum of a number of local pairings.

The set of bad primes of E is $P=\{2,3,5,19\}$, and in this case this set is not enlarged (see Proposition 3.3.6). The covering curves are provided by (8.2), and for each of our bad primes we find a local point on the covering curves. We used the ones in the following table.

Selmer group element	mod 2^2	mod 3^3	mod 5^2	mod 19^2
2	$(1:1:1:1:1)$	$(6:22:5:2:1)$	$(0:9:3:2:1)$	$(167:323:70:3:1)$
3	$(2:1:1:1:1)$	$(8:19:6:1:1)$	$(0:19:12:3:1)$	$(110:190:314:2:1)$
5	$(0:1:1:1:1)$	$(0:4:14:2:1)$	$(20:0:23:2:1)$	$(213:57:213:5:1)$

Each local pairing is calculated between the members of $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ and some other elements obtained by evaluating our pushout forms at these local points. The other elements thus obtained are given by the following tables, modulo fifth powers.

generator	mod 2^2	mod 3^3	mod 5^3	mod 19^2
2	$\zeta_5^2+\zeta_5$	$6\zeta_5^3+9\zeta_5^2+22\zeta_5+15$	$104\zeta_5^3+104\zeta_5^2+49\zeta_5+49$	$167\zeta_5^3+342\zeta_5^2$ $+285\zeta_5+305$
3	$\zeta_5^3+2\zeta_5^2+3$	$3\zeta_5^3+18\zeta_5^2+13\zeta_5+17$	$65\zeta_5^3+30\zeta_5^2+35\zeta_5+70$	$279\zeta_5^3+64\zeta_5^2$ $+145\zeta_5+90$
5	$3\zeta_5^3+2\zeta_5^2+2\zeta_5$	$14\zeta_5^3+14\zeta_5^2+18$	$5\zeta_5^3+38\zeta_5^2+65\zeta_5+70$	$10\zeta_5^3+324\zeta_5^2$ $+281\zeta_5+214$

We now use Section 3.2 to compute the local pairings. The primes 2 and 3 are inert in L, and 19 splits into two ideals. In all three cases, we will use part 6 of Proposition 3.2.6 to compute the pairing. Remember that by Remark 3.2.4, the final answer for 19 must be multiplied by 4. The following table gives the necessary information for the prime 2. Denote by $b_g^{(p)}$ the element obtained from Selmer generator g at prime p.

$(a, b_g^{(2)})_2$	$\mathrm{val}_2(a)$	$\mathrm{val}_2(b_g^{(2)})$	c	$\left(\frac{c}{2}\right)$
$(2, \zeta_5^2+\zeta_5)_2$	1	0	$3\zeta_5^2+3$	3
$(3, \zeta_5^2+\zeta_5)_2$	0	0	1	0
$(5, \zeta_5^2+\zeta_5)_2$	0	0	1	0
$(2, \zeta_5^3+2\zeta_5^2+3)_2$	1	0	$\zeta_5^2+3\zeta_5+3$	3
$(3, \zeta_5^3+2\zeta_5^2+3)_2$	0	0	1	0
$(5, \zeta_5^3+2\zeta_5^2+3)_2$	0	0	1	0
$(2, 3\zeta_5^3+2\zeta_5^2+2\zeta_5)_2$	1	0	$3\zeta_5^2+2\zeta_5+2$	1
$(3, 3\zeta_5^3+2\zeta_5^2+2\zeta_5)_2$	0	0	1	0
$(5, 3\zeta_5^3+2\zeta_5^2+2\zeta_5)_2$	0	0	1	0

Thus the local pairing at 2 is given by

	2	3	5
2	3	3	1
3	0	0	0
5	0	0	0

Similarly, the primes 3 and 19 give us the following information and matrices. The prime 3 is inert, but there are two primes lying over 19, and we choose to work with $p_{19} = -4\zeta_5^3 - 4\zeta_5^2 - 1$. By Remark 3.2.4 we must multiply the final matrix by 2 in this case.

$(a, b_g^{(3)})_3$	$\mathrm{val}_3(a)$	$\mathrm{val}_3(b_g^{(3)})$	c	$\left(\frac{c}{3}\right)$
$(2, 6\zeta_5^3+9\zeta_5^2+22\zeta_5+15)_3$	0	0	1	0
$(3, 6\zeta_5^3+9\zeta_5^2+22\zeta_5+15)_3$	1	0	$14\zeta_5^3+20\zeta_5^2+14\zeta_5+20$	4
$(5, 6\zeta_5^3+9\zeta_5^2+22\zeta_5+15)_3$	0	0	1	0
$(2, 3\zeta_5^3+18\zeta_5^2+13\zeta_5+17)_3$	0	0	1	0
$(3, 3\zeta_5^3+18\zeta_5^2+13\zeta_5+17)_3$	1	0	$25\zeta_5^3+17\zeta_5^2+22$	2
$(5, 3\zeta_5^3+18\zeta_5^2+13\zeta_5+17)_3$	0	0	1	0
$(2, 14\zeta_5^3+14\zeta_5^2+18)_3$	0	0	1	0
$(3, 14\zeta_5^3+14\zeta_5^2+18)_3$	1	0	$11\zeta_5^3+11\zeta_5^2+20$	0
$(5, 14\zeta_5^3+14\zeta_5^2+18)_3$	0	0	1	0

	2	3	5
2	0	0	0
3	4	2	0
5	0	0	0

$(a, b_g^{(5)})_{p_{19}}$	$\mathrm{val}_{p_{19}}(a)$	$\mathrm{val}_{p_{19}}(b_g^{(19)})$	c	$\left(\frac{c}{p_{19}}\right)$
$(2, 167\zeta_5^3+342\zeta_5^2+285\zeta_5+305)_{p_{19}}$	0	0	1	0
$(3, 167\zeta_5^3+342\zeta_5^2+285\zeta_5+305)_{p_{19}}$	0	0	1	0
$(5, 167\zeta_5^3+342\zeta_5^2+285\zeta_5+305)_{p_{19}}$	0	0	1	0
$(2, 279\zeta_5^3+64\zeta_5^2+145\zeta_5+90)_{p_{19}}$	0	0	1	0
$(3, 279\zeta_5^3+64\zeta_5^2+145\zeta_5+90)_{p_{19}}$	0	0	1	0
$(5, 279\zeta_5^3+64\zeta_5^2+145\zeta_5+90)_{p_{19}}$	0	0	1	0
$(2, 10\zeta_5^3+324\zeta_5^2+281\zeta_5+214)_{p_{19}}$	0	0	1	0
$(3, 10\zeta_5^3+324\zeta_5^2+281\zeta_5+214)_{p_{19}}$	0	0	1	0
$(5, 10\zeta_5^3+324\zeta_5^2+281\zeta_5+214)_{p_{19}}$	0	0	1	0

	2	3	5
2	0	0	0
3	0	0	0
5	0	0	0

We now move on the the final prime, 5, which is completely ramified in L. We must use Proposition 3.2.7. Each of the elements used lies in one of the classes generated by $\langle \lambda, \eta_1, \eta_2, \eta_3, \eta_4, \eta_5 \rangle$. The following table indicates which class each element is in.

element	class
2	$\eta_4^2\eta_5^4$
3	$\eta_4^4\eta_5^3$
5	$\lambda^4\eta_1^3\eta_2\eta_3$
$104\zeta_5^3+104\zeta_5^2+49\zeta_5+49$	$\eta_1^4\eta_4^2\eta_5^2$
$65\zeta_5^3+30\zeta_5^2+35\zeta_5+70$	$\eta_1^3\eta_5^3$
$5\zeta_5^3+38\zeta_5^2+65\zeta_5+70$	$\eta_1^2\eta_4^4\eta_5^3$

Using Table 3.2 we thus obtain the following matrix for the local pairing at 5.

	2	3	5
2	2	4	1
3	4	3	2
5	3	3	0

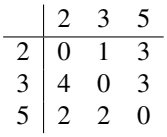
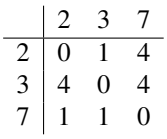
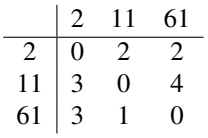
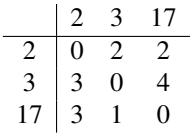
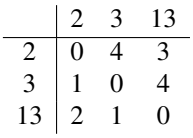
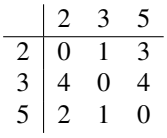
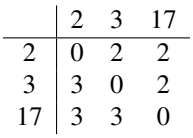
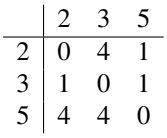
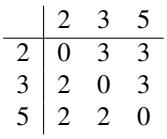
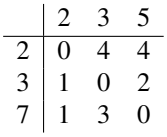
By adding up the four local pairings computed, we obtain the following matrix for the Cassels-Tate pairing.

	2	3	5
2	0	2	2
3	3	0	2
5	3	3	0

This is a rank 2 matrix, thus the rank of E must be 0 and we find that we have $Ш(\hat{E}/\mathbb{Q})[\hat{\phi}] \cong (\mathbb{Z}/5\mathbb{Z})^2$.

In the following table, λ is the parameter from Proposition 8.0.1. The conductor is given in the second column. The columns marked by $\mathscr{P}$ and $\mathscr{Q}\cup\mathscr{R}$ are the sets of primes obtained as in Section 2.6.2, which can be used to calculate a descent by 5-isogeny, as is shown in [Fis01]. The number r_ϕ indicates the rank after calculating a descent by 5-isogeny, and ϕ and $\hat{\phi}$ are the sizes of the Selmer groups $S^{(\phi)}(E/\mathbb{Q})$ and $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$ respectively. The matrix $\hat{M}$ is the matrix obtained by doing a Cassels-Tate pairing on the Selmer group $S^{(\hat{\phi})}(\hat{E}/\mathbb{Q})$, and r indicates the new upper bound for the rank in light of the rank of $\hat{M}$. The values of λ are taken from [Fis01, Table 1]

λ	N	$\mathscr{P}$	$\mathscr{Q}\cup\mathscr{R}$	$\hat{\phi}$	ϕ	r_ϕ	$\hat{M}$	$r(\hat{M})$	r
$\frac{48}{5}$	570	$\{2,3,5\}$	$\emptyset$	3	0	2	2: 0 2 2 3: 3 0 2 5: 3 3 0	2	0
$\frac{100}{9}$	570	$\{2,3,5\}$	$\emptyset$	3	0	2	2: 0 1 1 3: 4 0 1 5: 4 4 0	2	0
$\frac{45}{4}$	870	$\{2,3,5\}$	$\emptyset$	3	0	2	2: 0 2 1 3: 3 0 1 5: 4 4 0	2	0

$\frac{50}{3}$	870	$\{2,3,5\}$	$\emptyset$	3	0	2		2	0
$\frac{21}{2}$	1050	$\{2,3,7\}$	$\emptyset$	3	0	2		2	0
$\frac{122}{11}$	1342	$\{2,11,61\}$	$\emptyset$	3	0	2		2	0
$-\frac{68}{3}$	1938	$\{2,3,17\}$	$\emptyset$	3	0	2		2	0
$\frac{144}{13}$	1950	$\{2,3,13\}$	$\emptyset$	3	0	2		2	0
$\frac{54}{5}$	2370	$\{2,3,5\}$	$\emptyset$	3	0	2		2	0
$\frac{34}{3}$	2550	$\{2,3,17\}$	$\emptyset$	3	0	2		2	0
$\frac{15}{2}$	3270	$\{2,3,5\}$	$\emptyset$	3	0	2		2	0
$\frac{10}{3}$	7170	$\{2,3,5\}$	$\emptyset$	3	0	2		2	0
$\frac{98}{9}$	7518	$\{2,3,7\}$	$\emptyset$	3	0	2		2	0

$-\frac{3}{20}$	8070	$\{2,3,5\}$	$\emptyset$	3	0	2		2	0

	2	3	5
2	0	3	3
3	2	0	1
5	2	4	0

$-\frac{12}{133}$	8778	$\{2,3,7,19\}$	$\{11\}$	3	0	2		2	0

	12	76	133
12	0	1	0
76	4	0	4
133	0	1	0

Thus we see that the pushout form method generalises. We could also use this method for $p > 5$ if we so wished. The formulae for the pushout form would get very complicated, however after they have been computed, using them in calculations is not a heavy computational step and using them is simply a matter of plugging in various parameters. The bottleneck is the calculation of norm equations, which is an inevitable part of most of the methods for computing the Cassels-Tate pairing which we have explored in this thesis. This severely limits the use of the pushout form method in the cases $p > 3$.

Bibliography

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The MAGMA Algebra System: I The User Language. *J. Symbolic Comput.*, (24):235–265, 1997.

[Bel97] K. Belabas. A Fast Algorithm to Compute Cubic Fields. *Math. Comp*, 1997.

[BL04] C. Birkenhake and H. Lange. *Complex Abelian Varieties*. Springer-Verlag, 2004.

[BO13] G. Berhuy and F. Oggier. *Central Simple Algebras and Wireless Communications*. American Mathematical Society, 2013.

[Böl75] R. Bölling. Die Ordnung der Shafarewitsch-Tate Gruppe kann beliebig großwerden. *Math. Nachr.*, 67:157–179, 1975.

[Bra28] R. Brauer. Untersuchungen über die arithmetischen Eigenschaften von Gruppen linearen Substitutionen I. *Math. Zeit.*, (28):677–696, 1928.

[Bra30] R. Brauer. Untersuchungen über die arithmetischen Eigenschaften von Gruppen linearen Substitutionen II. *Math. Zeit.*, (31):733–747, 1930.

[Cas59] J.W.S. Cassels. Arithmetic on Curves of Genus 1, I. On a Conjecture of Selmer. *Reine Angew. Math.*, 202:52–99, 1959.

[Cas62] J.W.S. Cassels. Arithmetic on Curves of Genus 1, IV. Proof of the Hauptvermutung. *Reine Angew. Math.*, 211:95–112, 1962.

[Cas64] J.W.S. Cassels. Arithmetic on Curves of Genus 1, VI. The Tate-Shafarevich Group can be Arbitrarily Large. *Reine Angew. Math.*, 215:65–70, 1964.

[Cas65] J. W. S. Cassels. On the conjectures of Birch and Swinnerton-Dyer. *Reine Angew. Math.*, (217):180–199, 1965.

[Cas71] J.W.S. Cassels. *An Introduction to the Geometry of Numbers*. Springer-Verlag, 1971.

[Cas98] J.W.S. Cassels. Second Descents for Elliptic Curves. *J. reine angew. Math.*, 1998.

[CF67] J.W.S. Cassels and A. Frohlich. *Algebraic Number Theory*. Academic Press, 1967.

[CFO+08] J.E. Cremona, T.A. Fisher, C. O'Neill, D. Simon, and M. Stoll. Explicit n-descent on Elliptic Curves I: Algebra. *J. reine angew. Math.*, 615:121–155, 2008.

[CFO+09] J.E. Cremona, T.A. Fisher, C. O'Neill, D. Simon, and M. Stoll. Explicit n-descent on Elliptic Curves II: Geometry. *J. reine angew. Math.*, 632:63–84, 2009.

[CFO+12] J.E. Cremona, T.A. Fisher, C. O'Neill, D. Simon, and M. Stoll. Explicit n-descent on Elliptic Curves III: Algorithms. *Math. Comp.*, 84(292):895–922, 2012.

[Coh00] H. Cohen. *Advanced Topics in Computational Number Theory*. Springer-Verlag, 2000.

[CP09] H. Cohen and F. Pazuki. Elementary 3-Descent with a 3-Isogeny. *Acta Arithmetica*, 140(4):369–404, 2009.

[CR02] J.E. Cremona and D. Rusin. Efficient Solution of Rational Conics. *Mathematics of Computation*, 72(243):1417–1441, 2002.

[Cre99] J.E. Cremona. Reduction of Binary Cubic and Quartic Forms. *LMS Journal of Computation and Mathematics*, 2:62–92, 1999.

[Cre12] B. Creutz. Second p-Descents on Elliptic Curves. 2012.

[Cre15] J.E. Cremona. `http://www.lmfdb.org/`, May 2015.

[Dav45] H. Davenport. The Reduction of a Binary Cubic Form II. *J. London Math. Soc.*, (20):139–157, 1945.

[Del08] Matt Delong. A Formula for the Selmer group of a Rational Three-isogeny. In *ActaArith.105 (2002), 119-131. MR 2003i:11069*, 2008.

[Don] S. Donnelly. Computing the Cassels-Tate Pairing on X(E)[2] in MAGMA.

[DSS00] Z. Djabri, E.F. Schaefer, and N.P. Smart. Computing the p-Selmer Group of an Elliptic Curve. *Trans. Amer. Math. Soc.*, (352):5583–5597, 2000.

[Duj15] A. Dujella. `http://web.math.pmf.unizg.hr/ duje/tors/z3.html`, March 2015.

[EGM98] J. Elstrodt, F. Grunewald, and J. Mennicke. *Groups acting on Hyperbolic Space*. Springer-Verlag, 1998.

[Fis01] T. Fisher. Some examples of 5 and 7 descent for elliptic curves over $\mathbb{Q}$. *Eur. Math. Soc.*, (3):169–201, 2001.

[Fis03] T.A. Fisher. The Cassels-Tate pairing and the Platonic Solids. *Journal of Number Theory*, 98:105–155, 2003.

[Fis14] T. Fisher. Higher Descents on an Elliptic Curve with a Rational 2-Torsion Point. preprint 2014.

[FN14] T. Fisher and R. Newton. Computing the Cassels-Tate Pairing on the 3-Selmer Group of an Elliptic Curve. *Int. J. Number Theory*, 10(7):1881–1907, 2014.

[Gra03] G. Gras. *Class Field Theory: From Theory to Practice*. Springer-Verlag, 2003.

[GS06] P. Gille and T. Szamuely. *Central Simple Algebras and Galois Cohomology*. Cambridge University Press, 2006.

[Hus04] Dale Husemöller. *Elliptic Curves*. Springer, 2004.

[Jul17] G. Julia. étude sur les formes binaires non quadratiques á indéterminées réelles ou complexes. *Mem. Acad. Sci. l'Inst. France*, (55):1–293, 1917.

[Kub76] D. S. Kubert. Universal Bounds on the Torsion of Elliptic Curves. *Proc. London. Math. Soc.*, (33):193–237, 1976.

[Lin05] Mark Lingham. *Modular Forms and Elliptic Curves over Imaginary Quadratic Fields*. PhD thesis, University of Nottingham, 2005.

[LLL82] A.K. Lenstra, H.W. Lenstra, and L. Lovász. Factoring Polynomials with Rational Coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[LT58] S. Lang and J. Tate. Principal Homogeneous Spaces over Abelian Varieties. *American Journal of Mathematics*, (80):659–684, 1958.

[Mat12] G.B. Mathews. On the Reduction and Classification of Binary Cubics which have a Negative Discriminant. *Proc. London Math. Soc.*, 3(10):128–138, 1912.

[McG82] F.O. McGuinness. *The Cassels Pairing in a Family of Elliptic Curves*. PhD thesis, Brown University, 1982.

[Mer96] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, (124):437–449, 1996.

[Mor13] A. Morra. An Algorithm to Compute Relative Cubic Fields. *Math. Comp.*, 82(284):2343–2361, 2013.

[MS13] R.L. Miller and M. Stoll. Explicit Isogeny Descent on Elliptic Curves. *Math. Comp.*, (82):513–529, 2013.

[Ng95] K.O. Ng. The Classification of $(3,3,3)$-Trilinear Forms. *J. reine angew. Math*, (468):49–75, 1995.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*. Springer-Verlag, 2008.

[PS98] B. Poonen and M. Stoll. The Cassels-Tate Pairing on Polarized Abelian Varieties. *Ann. of Math*, 2:15–0, 1998.

[Rei86] M. A. Reichert. Explicit Determination of Nontrivial Torsion Structures of Elliptic Curves over Quadratic Number Fields. *Math. Comp.*, (46):637–658, 1986.

[Rot10] J. Rotman. *Advanced Modern Algebra*. American Mathematical Society, 2010.

[SC02] M. Stoll and J.E. Cremona. On the Reduction Theory of Binary Forms. 2002.

[Sel51] E.S. Selmer. The Diophantine Equation $ax^3 + by^3 + cz^3$. *Acta. Math*, (85):203–362, 1951.

[Ser79] J-P. Serre. *Local Fields*. Springer-Verlag, 1979.

[Ser02] J-P. Serre. *Galois Cohomology*. Springer, 2002.

[Sha59] I.R. Shafarevich. The Group of Principal Homogeneous Algebraic Manifolds. *Doklady Akademii Nauk SSSR*, (124):42–43, 1959.

[Sha98] E.F Shaefer. Computing a Selmer Group of a Jacobian using Functions on the Curve. *Math. Ann.*, 310(3):1209–1231, 1998.

[Sil08] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2008.

[Sim02] D. Simon. Solving Relative Norm Equations in Number Fields Using *S*-units. *Mathematics of Computation*, 71(239):1287–1305, 2002.

[SS03] E.F. Schaefer and M. Stoll. How to do a p-descent on an Elliptic Curve. *Transactions for the American Mathematical Society*, 2003.

[Tat74] J. Tate. The Arithmetic of Elliptic Curves. *Invent. Math.*, (23):176–206, 1974.

[Top91] J. Top. Descent by 3-isogeny and 3-rank of Quadratic Fields. In *Advances in number theory*, pages 303–317. Oxford Univ. Press, 1991.

[Vél71] J. Vélu. Isogénies entre courbes elliptiques. *C.R. Acad. Sci. Paries*, (A-B 273):A238–A241, 1971.